NETWORK ENABLED OPERATIONS: THE EXPERIENCES OF SENIOR CANADIAN COMMANDERS

A Report Prepared by

KMG Associates

Principal Authors:
BGen (retired) Joe Sharpe
Dr Allan English

Contract number: W7711-04-7908-04
Call-up number 7908-04

DRDC-Toronto Scientific Authority:
Keith Stewart
(416) 635-2000 x 2130

Defence R&D Canada - Toronto

Contract Report
DRDC Toronto CR 2006-112
31 March 2006

Authors

BGen (retired) Joe Sharpe

Dr Allan English

Approved by

Ms. Carol McCann

Section Head, Command Effectiveness & Behaviour

Approved for release by

K.M. Sutton
Chair, Document Review and Library Committee

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

ABSTRACT

In order to fully understand the nature of Networked Enabled Operations (NEOps) today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to provide context for and to document recent Canadian experiences with networked operations. However, to date, very little has been written on the Canadian experience with NEOps, particularly at the operational level of command. A recent DRDC Contract Report, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," provided some context for NEOps and noted that Canada has made significant contributions to the evolution of networked operations. It also noted that these contributions have not been well documented. This report begins the documentation of recent Canadian experiences with networked operations based on an analysis of interviews conducted during January and February 2006 with eight Canadian commanders who had recent experience with networked operations at the operational level of command. The analysis begins with a context for understanding NEOps; it then presents key issues raised in the interviews in a thematic format; and the analysis concludes by summarizing and synthesizing the key issues raised in the interviews.

RÉSUMÉ

Pour bien comprendre la nature actuelle des opérations facilitées par réseaux (OFR), la manière dont les opérations par réseaux menées par le Canada diffèrent de celles des autres pays et l'évolution possible des OFR, il est essentiel d'en définir le contexte et de recenser les récentes expériences du Canada en la matière. Toutefois, on a très peu écrit jusqu'à maintenant sur l'expérience canadienne dans ce domaine, en particulier au niveau opérationnel du commandement. Les auteurs d'un récent rapport contractuel de RDDC intitulé « *Attention de ne pas mettre la charrue devant les bœufs : les opérations réseaucentriques comme façon d'aborder la transformation au Canada*, » mettent les OFR en contexte et soulignent que le Canada a contribué de façon appréciable à l'évolution des opérations par réseaux. Ils ajoutent que peu d'études ont été faites au sujet de ces contributions. Dans ce rapport, on établit d'abord un dossier sur les récentes expériences du Canada liées aux opérations par réseaux, d'après une analyse des entrevues réalisées en janvier et en février 2006 auprès de huit commandants canadiens ayant récemment fait l'expérience de ces opérations au niveau de commandement opérationnel. Dans un premier temps, l'analyse définit le contexte pour comprendre les OFR; elle présente ensuite les principales questions posées au cours des entrevues thématiques, et se termine par un résumé et une synthèse de ces questions.

This page intentionally left blank

EXECUTIVE SUMMARY

Network Enabled Operations (NEOps) seems poised to become the driving concept behind CF transformation for a number of reasons, not the least of which is Canada's tendency to follow the American lead in new concepts related to war and other operations. To gain an understanding of NEOps as a professional tool, military professionals and others must be conscious of the historical and theoretical context in which it originated and is evolving. As part of this context, each nation and each service in a nation's armed forces have their own unique paradigm of how military operations should be conducted based on the physical environment in which they operate, their historical experience, and their culture.

NEOps as a concept has a promising future if it is predicated on Canadian needs and culture. However, there is significant risk in placing too much reliance on concepts like Network Centric Warfare which put the technological cart before the human requirements that should drive any transformation initiative. Therefore, future development of the NEOps concept should be firmly rooted in the Canadian context and based on Canadian experience.

However, to date, very little has been written on the Canadian experience with NEOps, particularly at the operational level of command. A recent DRDC Contract Report, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," provided some context for NEOps and noted that Canada has made significant contributions to the evolution of networked operations. It also noted that these contributions have not been well documented. This report begins the documentation of recent Canadian experiences with networked operations. It provides an analysis of interviews conducted during January and February 2006 with eight Canadian commanders who had recent experience with networked operations at the operational level of command. The commanders interviewed were BGen P.J. Devlin, Vice-Admiral J.C.J.Y. Forcier, Rear-Admiral R. Girouard, BGen J.P.Y.D. Gosselin, Commodore (Retired) Eric Lerhe, MGen W.J. Natynczyk, Col P.B. Stogran, and BGen D.C. Tabbenor.

The analysis begins with a context for understanding NEOps; it then presents key issues raised in the interviews in a thematic format; and the analysis concludes by summarizing and synthesizing the key issues raised in the interviews. The key conclusions are summarized next.

Different interpretations of the meaning of terms associated with networked operations. There was consensus among those interviewed that there are many different interpretations of terms associated with networked operations. However, there was no consensus among them on the precise meanings of these terms. All those interviewed agreed that networked operations were going to be an important part of future military missions; therefore, they recognized the need to work towards a common understanding of what networked operations means in different contexts.

Differences in how networked systems are used. One of the problems with achieving a common understanding of networked operations is that there is no standard model for a networked system, because different missions and different operating environments require

different types of networks. Despite the differences in networked systems, almost all of those interviewed commented on the need to establish trust among those working in an operation through face-to-face contact.

The effect of networks on command. Those interviewed had differing views on how the use of networks affected how command was exercised in operations. Most of those interviewed believed that human networks created through human relationships are critical to effective operations and, while technical networks are essential to support the human networks, the technical networks must be used in such a way that they enable rather than detract from the exercise of command.

The need for both human networks and technological networks, and the relative value of each. All of those interviewed recognized that both human networks and technological networks were required in today's operations. They also agreed that the technical network should enable the human network. However, how the technical network could enable the human network will vary according to circumstances. Most found that one of the key functions of the human system is to find ways to compensate for technical, doctrinal and training disparities among members of organizations in the network.

The potential for networks to encourage "micromanagement" interference in the chain of command. What style of leadership or command is most appropriate for networked operations? One specific effect of networks on the chain of command raised by all those interviewed, but expressed in different ways, was that networks could encourage higher levels of command to micromanage lower levels of command.

Virtually all of those interviewed agreed that mission command was the preferred command philosophy for networked operations; however, many observed that environmental (or service), cultural and individual differences in interpreting how that philosophy should be applied in practice caused problems in networked operations.

The challenge of Canadians conducting networked operations with partners with different technological capabilities. The challenges of conducting networked operations with partners, including OGDs and NGOs, with different technological capabilities are unlikely to change significantly in the foreseeable future. In developing concepts for networked operations in this country it should be clear that "one size does not fit all," because the needs for sophisticated technical networks among the environments in the CF can vary almost as much as the needs among coalition partners, according to those interviewed.

Competencies required by senior commanders to manage both the technical and the human dimensions of network-enabled systems. Commanders must have an awareness of both the technical and the human dimensions of network-enabled systems in order to effectively command in a networked environment, according to those interviewed.

Most of those interviewed felt that humans had the ability to overcome most of the problems described in this section. But to overcome these problems, those working with networked systems need the competencies to understand where they fit into both the human and the technical networks, and then they need to have leaders who will let them use their initiative to meet the challenges of working in a networked environment.

This page intentionally left blank

SOMMAIRE

Les opérations facilitées par réseaux (OFR) semblent sur le point de devenir le concept moteur derrière la transformation des Forces canadiennes (FC) pour un certain nombre de raisons, dont la tendance du Canada à suivre la direction américaine dans les nouveaux concepts liés à la guerre et à d’autres opérations n’est pas la moindre. Pour comprendre l’outil professionnel que constituent les OFR, les professionnels militaires et les autres intervenants doivent être bien conscients du contexte historique et théorique qui en est à l’origine et dans lequel elles évoluent. Dans ce contexte, chaque pays et chaque service de ses forces armées possède son propre paradigme quant à la manière de mener les opérations militaires en fonction de l’environnement physique, de son expérience historique et de sa culture.

En tant que concept, les OFR ont un avenir prometteur si elles reposent sur notre culture et nos besoins. Cependant, il y aura un risque important à trop dépendre de concepts comme la guerre réseaucentrique, par exemple, qui met la charrue de la technologie devant les exigences humaines qui devraient diriger toute initiative de transformation. Par conséquent, l’élaboration future du concept des OFR devrait être solidement ancrée dans le contexte canadien et axée sur l’expérience canadienne.

Toutefois, on a très peu écrit jusqu’à maintenant sur l’expérience canadienne dans le domaine des OFR, en particulier au niveau opérationnel du commandement. Les auteurs d’un récent rapport contractuel de RDDC intitulé « *Attention de ne pas mettre la charrue devant les bœufs : les opérations réseaucentriques comme façon d’aborder la transformation au Canada*, » mettent les OFR en contexte et soulignent que le Canada a contribué de façon appréciable à l’évolution des opérations par réseaux. Ils ajoutent que peu d’études ont été faites au sujet de ces contributions. Dans ce rapport, on établit d’abord un dossier sur les récentes expériences du Canada liées aux opérations par réseaux. On y analyse également les entrevues réalisées en janvier et en février 2006 auprès de huit commandants canadiens ayant récemment fait l’expérience de ces opérations au niveau de commandement opérationnel. Les commandants interrogés sont le Bgén P.J. Devlin, le Vice-amiral J.C.J.Y. Forcier, le Contre-amiral R. Girouard, le Bgén J.P.Y.D. Gosselin, le Commodore (retraité) Eric Lerhe, le Mgén W.J. Natynczyk, le Col P.B. Stogran, et le Bgén D.C. Tabbenor.

Dans un premier temps, l’analyse définit le contexte pour comprendre les OFR; elle présente ensuite les principales questions posées au cours des entrevues thématiques, et se termine par un résumé et une synthèse de ces questions. Les principales conclusions sont résumées ci-après.

Différentes interprétations des expressions associées aux opérations par réseaux. Les militaires interrogés sont unanimes à reconnaître que les expressions associées aux opérations par réseaux font l’objet de maintes interprétations différentes. Toutefois, il n’y a pas d’accord entre eux sur le sens précis de ces expressions. Tous conviennent que les opérations par réseaux vont représenter une part importante des missions militaires de l’avenir, et reconnaissent donc la nécessité de parvenir à une interprétation commune des opérations par réseaux dans différents contextes.

Différences dans l’utilisation des systèmes réseau. L’un des obstacles pour en arriver à une vue commune des opérations par réseaux est l’absence d’un modèle type de système réseau, car des missions différentes et des cadres d’exploitation différents nécessitent des types de réseaux différents. Malgré les divergences entre les systèmes réseau, la plupart des commandants interrogés font valoir la nécessité d’établir un lien de confiance au moyen d’un contact personnel entre ceux qui collaborent à une opération.

L’effet des réseaux sur le commandement. Les militaires interrogés perçoivent différemment la manière dont l’utilisation des réseaux influe sur l’exercice du commandement au cours des opérations. La plupart estiment que les réseaux humains créés par le biais des rapports entre les personnes sont essentiels à l’efficacité des opérations, et même si les réseaux techniques sont essentiels au soutien des réseaux humains, les réseaux techniques doivent être exploités de manière à faciliter l’exercice du commandement plutôt qu’à l’entraver.

La nécessité des réseaux humains et des réseaux technologiques, et leur valeur les uns par rapport aux autres. Les commandants interrogés reconnaissent que les opérations actuelles nécessitent à la fois des réseaux humains et des réseaux technologiques. Ils sont aussi d’avis que le réseau technique devrait faciliter le réseau humain, mais la manière d’y arriver varie selon les circonstances. Pour la plupart, l’une des principales fonctions du système humain consiste à trouver des moyens de compenser les disparités entre les membres des organisations du réseau, des points de vue de la technique, de la doctrine et de l’instruction.

Le potentiel des réseaux d’encourager une interférence de « microgestion » dans la chaîne de commandement. Quel style de leadership ou de commandement convient le mieux aux opérations par réseaux? L’un des effets particuliers des réseaux sur la chaîne de commandement, mentionné par tous les commandants interrogés mais exprimé différemment, est que les réseaux pourraient encourager les niveaux supérieurs de commandement à microgérer les niveaux de commandement subordonnés.

Pratiquement tous les commandants consultés reconnaissent que le commandement de mission est la philosophie de commandement à privilégier pour les opérations par réseaux; toutefois, pour beaucoup d’entre eux, les différences liées à l’armée (ou au service) ou d’ordre culturel et individuel dans la manière d’interpréter l’application pratique de cette philosophie posent problème au niveau des opérations par réseaux.

Le défi, pour les Canadiens, de mener des opérations par réseaux avec des partenaires dotés de capacités technologiques différentes. Les défis à relever au cours des opérations par réseaux menées avec des partenaires, y compris d’autres ministères et des ONG, ayant des capacités technologiques différentes ne changeront probablement guère dans un avenir prévisible. Il ne devrait faire aucun doute, dans l’élaboration des concepts d’opérations par réseaux dans ce pays, qu’il n’y a pas de solution universelle car, selon les commandants interrogés, les besoins en réseaux techniques perfectionnés peuvent varier quasi autant entre les diverses armées des FC qu’entre les partenaires de coalition.

Compétences dont les commandants supérieurs ont besoin pour gérer à la fois les dimensions techniques et humaines des systèmes facilités par réseaux. D’après les personnes consultées, les commandants doivent être au courant des dimensions techniques et humaines des systèmes facilités par réseaux pour bien exercer leur commandement dans un environnement par réseaux.

En effet, la plupart sont d'avis que les humains sont en mesure de surmonter la plupart des problèmes décrits dans cette partie. Mais pour y arriver, les utilisateurs des systèmes par réseaux ont besoin de compétences pour comprendre leur position dans les réseaux humains et techniques, et de chefs qui leur laissent l'initiative pour relever les défis du travail dans un environnement par réseaux.

This page intentionally left blank

TABLE OF CONTENTS

INTRODUCTION

The concept of Networked Enabled Operations (NEOps) is central to the Transformation of the CF that is now being undertaken. The NEOps concept is emerging through discussions and papers within Defence Research and Development Canada (DRDC) and jointly with other players in the Department of National Defence (DND). A particular concern of DRDC Toronto in this regard is the critical human factors implications of NEOps and the establishment of a research agenda to address them.

To date very little has been written on the Canadian experience with NEOps, particularly at the operational level of command. A recent DRDC Contract Report, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," noted that Canada has made significant contributions to the evolution of networked operations, but that these contributions have not been well documented.[1] In order to fully understand the nature of NEOps today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to document recent Canadian experiences with networked operations.

This report addresses a requirement for in-depth understanding and documentation of recent Canadian experience with networked operations. It aims to contribute to the on-going development of NEOps concepts and capability in Canada. The paper provides a context for the experience of these commanders, compares the nature of networking in the various contexts, outlines both positive and negative aspects of networking and provides conclusions about how these experiences have contributed to the emerging theory of Networked Enabled Operations in the CF.

METHOD

The following activities were conducted to achieve the aims of this project.

1. A protocol was prepared for interviewing commanders about their experiences in networked operations, and the protocol was revised based on discussions with the SA. The protocol was submitted to the DRDC Toronto Research Ethics Board (REB) and it was approved on 5 Dec 2005. The REB submission with the protocol is at Annex A to this report.

2. During Jan and Feb 2006 eight Canadian commanders, who had recent experience with networked operations at the operational level of command, were interviewed and transcripts of the interviews were made. The commanders interviewed were BGen P.J. Devlin, Vice-Admiral

[1] Allan English, Richard Gimblett, and Howard Coombs, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," DRDC Toronto, Contract Report CR 2005-212 (19 July 2005).

J.C.J.Y. Forcier, Rear-Admiral R. Girouard, BGen J.P.Y.D. Gosselin, Commodore (Retired) Eric Lerhe, MGen W.J. Natynczyk, Col P.B. Stogran, and BGen D.C. Tabbenor. The biographies of those interviewed are at Annex B.

3. This paper was prepared based on an analysis of the interviews and transcripts of the interviews by subject matter experts (SMEs). The SMEs were Mr Howard Coombs, Dr Allan English, Dr Richard Gimblett, and BGen (retired) Joe Sharpe.

DISCUSSION

Context

Network Enabled Operations (NEOps) seems poised to become the driving concept behind CF transformation for a number of reasons, not the least of which is Canada's tendency to follow the American lead in new concepts related to war and other operations. Even though NEOps has not yet been clearly defined, recent NEOps conceptual statements indicate a similarity to the American concept of Network-Centric Warfare (NCW) as NEOps is expected "'to generate increased combat power by networking sensors, decision makers and combatants to achieve shared battlespace awareness, increased speed of command, higher operational tempo, greater lethality, increased survivability, and greater adaptability through rapid feedback loops.'"[2]

Many believe that in order to adapt to change through innovation, military professionals and those in the defence community need to understand the intellectual as well as the technical tools that they use in their work. To gain an understanding of NEOps as a professional tool, they must, therefore, be conscious of the historical and theoretical context in which it originated and is evolving. As part of this context, it was noted that each nation and each service in a nation's armed forces have their own unique paradigm of how military operations should be conducted based on the physical environment in which they operate, their historical experience, and their culture.

These physical and cultural settings in which armed forces operate form the basis for a number of critiques of NCW, whose advocates propose a specific type of command-by-influence, or mission command, as a key to future networked operations based on NCW. As noted in this report, this "one size fits all" approach to command may not work in today's varied operating environments. For example, air forces operate in the least cluttered battlespace. In these circumstances both command-by-direction and command-by-plan are possible, and they are effective command styles given the nature of modern air warfare. Armies, on the other hand, usually operate in the most complex and chaotic operating environment, and, therefore Western armies have, for the most part adopted the doctrine of mission command or command-by-influence so that decisions can, in theory, be taken by those closest to the situation, often down to the level of the individual soldier. Navies, however, operate in an environment of medium

[2] Michael H. Thomson and Barbara D. Adams, "Network Enabled Operations: A Canadian Perspective," (Defence Research and Development (DRDC) - Toronto contract report CR-2005-162, 13 May 2005), 5.

complexity, compared to air forces and armies, and, therefore most Western navies in the Anglo-American command tradition have identified the need for a command and control system to effectively coordinate maritime operations in a relatively complex, multi-threat environment, over a wide area. Within the naval framework, although individuals would be connected via their consoles, they would be operating as elements of larger systems, such as the various ships' operations rooms (at the lowest level) within the fleet framework. While the Canadian Navy and some other navies in the Anglo-American command tradition are creating and increasingly implementing a unique naval command-by-influence style, navies still have occasion to use the command-by-direction style that they have practised for centuries.

Despite working in different physical environments with different command and technical systems, the Canadian naval and land force experience, particularly the Army's stabilization efforts in post-conflict Afghanistan and the Navy's command of coalition operations in the Arabian Sea, reinforces the belief that the human network, not the technical network, should be the basis for future approaches to CF transformation. However, the differences in the physical environments among land, sea and air forces often dictate different approaches to conducting operations that in turn demand different command arrangements and technical systems. Therefore, a "one size fits all" approach to command and control may not be the best solution for networked operations, even in an increasingly integrated joint and combined operating environment.

NEOps as a concept has a promising future if it is predicated on Canadian needs and culture. However, there is significant risk in placing too much reliance on concepts like NCW which put the technological cart before the human requirements that should drive any transformation initiative. Therefore, future development of the NEOps concept should be firmly rooted in the Canadian context and based on Canadian experience. NEOps concept development should be complemented by the relevant experience of others, but it should avoid slavishly copying other frameworks as DND has sometimes done in the past. In the Canadian context of human-centred networks, research to support the development of the NEOps concept should be conducted in the areas related to the human dimension of networks based on theory and on Canadian practical experience. In this way, NEOps could become a suitable model to support the transformation of the CF and DND. By capturing the views of eight Canadian commanders, with recent experience with networked operations at the operational level of command, these interviews are one step in this research process. [3]

Themes from the Interviews

The following themes emerged from a review of NEOps interviews.

1. Different interpretations of the meaning of terms associated with networked operations.

The assertion in the "Beware of Putting the Cart before the Horse" that NEOps as a concept has not yet been clearly defined is supported by comments from those interviewed, particularly

[3] This section of the report is based on English, et al., "Beware of Putting the Cart before the Horse."

Devlin and Stogran, who suggested that current definitions were not being driven by user requirements. Forcier offered a different perspective. He argued that "…we don't think of network centric warfare anymore. It is just one of the tools that we have…an enabler."

Gosselin offered this definition of NEOps – the ability to make better decisions at all levels, faster and more accurately despite the fog of war. He elaborated on this definition with these remarks "[NEOps gives] the ability to share information in order to … enable better combat effects. …quicker, faster, decision time at every level. …the centrality of all this should be decision making. It should be about being able to make better, faster decisions. It could be a shooter who has the ability to quickly know the situation and whatever degree of accuracy he needs to take a decision to put some iron on a target or a commander who, in the fog of operations, is able to take better decisions, faster…it's the only issue."

Devlin said that the idea of networked operations is a very "complex issue that has not been solved" to the satisfaction of the users. He went on to say that he saw a great deal of similarity between the terms NCW and NEOps but that he preferred the term NEOps because it had more potential in current and future operations. For Devlin the term NCW had two main failings in its terminology. The first is the term network-centric because it implied "that everything is centred on the network, and so if there are failings there, there will be huge failings." The second is the term warfare because today's operations encompass much more than warfare. For example, the CF is now pursuing the idea of integrated operations which advocates achieving desired effects through co-ordinated actions by many different agencies, such as the military, police forces, other government departments (OGDs) and non-governmental organizations (NGOs).

He noted that the Provincial Reconstruction Teams (PRTs) in Kandahar, Afghanistan had "the Canadian military working along side Foreign Affairs, along side CIDA, along side some economic development folks, maybe some Treasury Board folks, maybe some infrastructure folks." Therefore, all those in this network could "share the information that's necessary for them to be able to make decisions, give some direction and then assess the results of that direction."[4] Devlin believed that this type of model might have applications in many other areas where integrated operations are envisioned. He concluded that: "Network Enabled Operations is all about sharing, having access to, providing direction, and assessing the results of that direction to those folks that need it." Stogran agreed with Devlin that the term "warfare" in NCW was too limiting and he stressed that it was essential to have connectivity at every level of the military and Canadian government, but that insight into the issues and common intent at every level was also critical.

There was consensus among those interviewed that there are currently many different interpretations of terms associated with networked operations. Those interviewed also agreed that networked operations were going to be an important part of future military missions; however, almost everyone recognized the need to be able to work towards a common understanding of what networked operations means in different contexts.

[4] See Coombs & Hillier

2. Differences in how networked systems are used.

One of the problems with defining various terms associated with networked operations, like NCW and NEOps, is that there is no standard model for a networked system and different missions and different operating environments require different C2 arrangements, and, therefore different types of networks. As noted in the paper "Beware of Putting the Cart before the Horse," van Creveld's dictum that, "one size does not fit all" in C2 systems, seems to be true.

For example, Devlin described his experiences in Afghanistan in 2003, working with 24 nations, as a limited NEOps environment. He found that "the staff [became] very reliant on the network as a means to be able to pass info and pass direction." He said that the staff worked hard "to achieve reasonable positional awareness," but that the network did not have the capability to increase positional awareness to situational awareness, and that intent could not be shown on the display. This was a significant challenge, according to Devlin, because he believed that limited networks, like the one used in Afghanistan in 2003, required strong "people skills" to create the relationships necessary to build common intent that was critical to exploiting the limited network that was available. For example, with intelligence information, the commander wanted more than just data; he wanted an assessment of the data. Devlin found that establishing trust was key to accepting an intelligence assessment, and that personal relationships and command relationships were key to building trust, especially because the nature of the threat, and, therefore the nature of missions, had changed significantly in the post-9/11 world. He put it this way, "It was important to look folks in the eyes and be able to relay how important this change was and what the mission was…" Devlin said that looking people in the eyes was vital in a multinational environment, and that back briefs and giving orders face-to-face was critical to the success of the mission.

Girouard echoed Devlin's comments: "It is about trust. It is about getting out there, certainly as a Mission Commander, getting out there and looking [in] your bosses' eyeballs and getting out there and doing that wonderful Nelsonian thing, looking in the eyeballs of your Captains." This personal contact enables commanders to talk about issues and concerns frankly in ways that would not be possible in message form or even in "chat" on the internet. With the pace and the risk (including political risk) involved in today's operations, he added, "trust matters more today than it ever has…"

Sometimes technical systems, like videoconferencing, can be used to build trust. Tabbernor, who was far removed from the operational theatre for which he had responsibility, found that the absence of a video teleconferencing (VTC) capability in his command inhibited the development of strong personal networks based on trust. In his view, while telephone communications were adequate, not having that a VTC capability was an impediment to being as effective as possible. He added that, while VTC is better than phone communications, the best way to build trust and common intent is by face-to-face communications. Because Tabbernor only went into theatre about once every five weeks he found that the lack of face-to-face communications caused misunderstandings between the various levels of command - tactical, operational, and strategic. He went on to say that misperceptions among the levels of command "had a huge impact on the people on the ground" in theatre. He cautioned that over-reliance on technologically-based systems can have very negative effects on the people on the ground, and that his experience was that an over-reliance on technology in this case, “had a very negative impact on…the operation. And the impact was on people. It was a very, very negative impact in a number of cases.”

Gosselin stressed the importance of working with a team of people that is known to the commander to ensure that commander’s intent is well communicated. He argued that it is easier to establish common intent in the early stages of an operation, and if the team is made up of people who have worked together with each other and with the commander before, common intent is established more quickly.

Stogran argued that the Americans use information operations to fight in the physical domain, to enhance their decision-making capabilities so they can give sensor-to-shooter information to those on the ground. The terrorists, on the other hand, he says, “are using information to affect the physical domain.” The difference, according to Stogran, is that terrorists are using information to enable human networks, whereas Western militaries tend to use information to maximize the physical effects of weapons. He argued that “we should be thinking more like terrorists” and be using technical systems to enable human networks.

Natynczyk was more comfortable, based on his experience, working with networked systems. He gave the example of the US Army Battle Command System, which took inputs from many different sources and provided the commander with not only information, but also the context of a situation. He claimed that using this particular command system allowed the commander to achieve “predictive intuition” of the situation and that this intuition allowed him to know where to focus his attention. An awareness of where to focus his attention then enabled the corps commander to deal personally with a divisional commander or a brigade commander or even a battalion commander, but at the same time, “not lose the bubble of what’s happening on the flanks” or in the rear “which can all reach out and bite.” He felt that a major advantage of networked operations as practiced by the US Army was that “…now the senior commander can see this incredibly complex theatre” and, when necessary, focus on just a few elements or indicators that “could really turn the tide between success and failure.” Natynczyk noted that network technology “facilitates the collection of … ‘Actionable Metrics’ … performance measurement tools that you can now apply based upon all of the inputs from the technology … to be able to see what kind of attacks were occurring [and] when.” Actionable Metrics allowed the US Army in Iraq to establish trends and to see how the enemy changed tactics. These metrics were then used to plan a response to the enemy.

Natynczyk gave an example of using Actionable Metrics at the section and platoon level from his experience in Iraq where “in six hours from the first incident soldiers changed their tactics, techniques and procedures because the enemy [had] adjusted their attack profiles.” In this example soldiers had been removing posters of Saddam Hussein as they had been told to remove any open signs of support for him. At one point it was found that plastic explosives were being put behind these signs which were severely injuring those removing the signs. After only a couple of cases of these booby trapped signs, junior leaders immediately got on to the tactical “chat room” to make that information available, and “within six hours that observation had been validated and … direction was put out that if you saw this kind of thing, do not touch the posters, call the explosive ordinance disposal people…and they would remove it.”

However, Natynczyk noted that in the CF there has been resistance to technology based on the culture of Canada's military. He observed that in the early 1990s, when email had just become available to computers on every desk, "people did not trust the email system. And it wasn't until Canadian general officers started sending their emails out that subordinates had to hoist aboard the importance of this new technology. There was the classic aversion to change. And that's the same with every organization…Until they understand that the new technology enables them better than their old practices…[then] they all sign up."

Forcier worried that some in the CF still see network-centric or network-enabled operations "as being more dots on the screen and less background information." He expressed some frustration with the current evolution of CF doctrine and processes because "we've become fascinated with dots on the screen…the network-centric approach of yesterday [that is] still permeating our system today is a simplistic view of quantitative versus qualitative" information. In other words, some still are working to increase the volume of information on the network without much regard for its quality. Forcier went on to say that "…the biggest challenge…I have to be quite candid, is that there still is a huge number of people in Ottawa that are looking at dots. And I'm looking at information…and…that's my challenge in using network-enabled philosophy in the Canadian context because people are happier to see dots on the screen."

3. The effect of networks on command.

Those interviewed had differing views on how the use of networks affected how command was exercised in operations. Tabbernor found that distance between the Canadian operational-level headquarters (co-located with CENTCOM in Florida) and the theatre of operations, the Middle East, had a negative effect on the chain of command that could only be partially mitigated by technical networks. Tabbernor noted that, in accordance with the doctrine of mission command, he "only went into theatre about once every five weeks" because he did not want to appear to be interfering in the tactical level of command. But, as noted above, the lack of face-to-face communications caused misunderstandings between the various levels of command.

While, on one hand, information available on the net could help to overcome the lack of personal contact among members of the human network, on the other hand the availability of information could also undermine the authority of the chain of command. Because some information could "be pulled down by everyone interested in the subject, and is available to all at the same time," situations arose where subordinates were aware of an issue before the commander. This was particularly true in cases where strategic-level staffs had promulgated policies without consulting the operational-level commander. In Tabbernor's opinion, these situations could contribute to a loss of authority for the chain of command. He said this loss of authority had the "potential to have a negative impact on the soldiers" because the commander's subordinates assumed that the commander was aware of the policy changes and had been consulted about them; however, the commander was "finding out about it at the same time as the soldier." This resulted in situations where subordinates were "poking you in the chest saying 'why are we doing this?'" and the commander could only answer "I don't know! I read it just the same time you did."

Tabbernor echoed the sentiments of many of those interviewed when he suggested that the solution to this problem was to continue to develop and intelligently use the human network as well as the technical one, because officers and NCOs in the chain of command are the ones who eventually have to explain policies to the soldiers. Therefore, the leadership in the chain of command needs to know before their subordinates about impending policy changes. However, Tabbernor worried that if the DND administrative bureaucracy forgets the leadership role of the commander and the CF becomes too reliant on technological aspects of the network, forgetting the importance of face-to-face communication in any network, then this reliance on technology could "undermine the soldiers' respect for the chain of command and their leaders."

Networked environments can, however, be used to enhance a commander's intent if it is well articulated and well understood. When forces are dispersed, such as Canadian units in Operation Apollo with the headquarters in Florida and troops in the Persian Gulf region or Afghanistan, technology was critical to maintaining close contact with those units. But the human dimension of command based on commander's intent was also critical. Tabbernor put it this way, "…once everybody understands the commander's intent … technology can be used to control the operation…command is one commander talking to another commander saying 'This is what I want.' And the commander going back to his boss saying 'Yeah, I understand what you want.'" Technological networks can use devices like VTC to enhance commander's intent, but "Just like the staff are tools to support the commander…"

However, sometimes the potential for the exchange of information provided by networks can make it difficult for commanders to articulate their intent over the volume of other information on the network. This difficulty was noted by commanders who used networked systems in a naval environment when dealing with subordinates who had difficulty differentiating "chat" from direction on the network. This became evident to Lerhe and Girouard when they found that, with the growing use of network-enabled operations, some subordinates lacked the ability to distinguish among situations where the network was used as an information sharing "chat" line and when it became a medium to transmit direction. There were differences of opinion among those interviewed on how to deal with this problem.

Lerhe expressed his concern about the difficulty that some subordinates had in distinguishing between "chat" and direction on a network, despite the existence of very clear procedures to distinguish between the two. [5] He found, nevertheless, that some commanding officers were unable to distinguish between the two because their previous experience and cultural background did not prepare them for this situation, and they expected orders to be clearly separated from "chat."

Girouard agreed that this problem existed, but he described how he dealt with it. He acknowledged that the Force Commander used the network both to exchange information in a "chat" scenario and to issue orders. This practice sometimes raised the question among subordinates - "so are those orders or are they not?" Therefore, he established a protocol where the Force Commander would use chat to give orders, but that orders would also be confirmed in a separate message. The confirmatory orders message would then be repeated in various other

[5] The procedure involved preceding an actual order with the term "This is CZ" –the commander's call sign and ending the transmission with the date time group - 211324Z.

formats and this gave the orders “tremendous on-going repeated visibility.” Despite the success of this protocol, Girouard always had the ability to deal with a sudden crisis by going on chat and saying “ ‘orders’ and when an officer or CO saw that on his screen ‘orders from me’ they understood that that wasn’t just conversational anymore. It was firm guidance. This was the equivalent of a signal directive. But, I’d always back it up again [with a confirmatory orders message].”

In summary, the existence of a fully functioning network-enabled environment does not negate the need for more human networks that are enabled by human relationships built on trust fostered by face-to-face meetings. Furthermore, the technological network must be used in such a way that it enables rather than detracts from the chain of command.

4. The need for both human networks and technological networks, and the relative value of each.

The majority of those interviewed were concerned that the significance of the human network not be lost when developing concepts of networked operations. Tabbernor pointed out that in countries like Afghanistan, that do not have sophisticated technological networks, human networks and the people skills necessary to develop these human networks are more important than the technological networks. Tabbernor also noted that if the mission of the military is to maintain contact with a wide range of organizations, like OGDs and NGOs, that have different levels of technological skills and sophistication, then the military must be aware of these differences and be prepared to deal with the technological lowest common denominator: “… in a lot of cases, the NGOs that you’re dealing with [don’t] necessarily have the same technology that we have. So they might have access to the World Wide Web through a computer site, but that might be it. They might have cell phones; they might not, depending on how wealthy the NGO is…I think when you’re dealing with your allies you have to look at what is the lowest common denominator that allows you to have effective communications with your allies, the governmental and non-governmental organizations.”

In Tabbernor’s opinion, it is critical to establish a balance between human networks and technical networks, ensuring that the technical network remains a tool: “I don’t think we can afford dollar-wise to emulate the Americans. So I think there needs to be a comfortable balance between the technical and the human. And to me the technical aspects are just a tool for the humans to use. And if we become too reliant on the technical I think we’re putting ourselves at risk.”

Girouard spoke emphatically of the importance of both types of networks because each network had characteristics that were important to supporting commanders in executing their missions. However, this commander felt that the human network was “a bit more important” because, the human network was the basis for establishing trust, which is the foundation for putting technology to work. The technical network then facilitates that trust by providing information and timely tactical data. Natynczyk supported the view that both types of networks were important because commanders needed the technology to enable command: “…[command is] not the technology. And it’s not the boxes…It’s what happens to the Commander inside his head. …The Commander … now can see what’s happening. That allows him the intuition. …So he

knows exactly when to say to that subordinate Commander - ‘Move now. The conditions are right. I’ve shaped your success.’”
The importance of the human dimension of the network was reinforced by Tabbernor, who said that knowing the source of the information is less important than knowing and trusting the individuals who are responsible for posting the information on the network. He elaborated on this idea as follows: “I don’t think that the commander needs to know the source, but the people who bring in the information should have verified the source.” Girouard took issue with this approach and argued that, for him, knowing the source of information is critically important and would have an impact on the risk he was willing to take in a given situation: “I have … a very healthy cynical streak about where [information comes] from.” When subordinates give the source of information as “‘they said’ I’m very much inclined to say who is ‘they’?...Who got this [information]?...it’s an important issue and it’s an aspect that I think we need to embed in the psyche of our people as we go down this wonderful technological road and particularly for our young generation that isn’t as accustomed to analytical thought processes.” Natynczyk agreed that relationships were important in assessing the value of intelligence and that commanders had to be able to speak to subordinate commanders face-to-face “to put the circumstances into context.” Natynczyk also reinforced the importance of technology in helping “commanders to understand the context of what they are doing…in the midst of an incredibly complex and diverse and ever-changing battlefield.”

Devlin believed that both human networks and technological networks were important because “great strength” comes from each. He noted that it was important for a joint force commander to create and maintain common intent among his “leadership team and the staff at the HQ,” and that technology could assist in this task. For example, the network could be used to pass information to those involved in the mission to prepare them for face-to-face meetings so that these meetings would not be wasted exchanging routine information, and could instead deal with more substantive issues. Once trust and common intent was established, technological means could be used to help maintain trust and common intent. For example, VTC, or more recently Voice over Internet Protocol (VoIP),[6] have made it easier for commanders to maintain trust and common intent with their subordinates. Devlin said that VoIP “has awesome capability for the bandwidth that it uses for a commander to jump on his network and to be able to have a voice conversation with his other commanders … he can do that with [VoIP] with great quality…”

Devlin concludes that technology should be an enabler because “The military will always be a people-oriented business, so relationships will remain vital… I just think you need to be able to strike the balance to exploit the wonderful power from technology that is out there and grows every day with one’s ability to influence people and build relationships and understanding.”

Stogran reinforced Devlin’s message noting that the rigidity of technical systems can limit their usefulness and asserting that, “Ultimately, on the end of these [technical] networks are human beings. If you rely too much on the [technical] network, it becomes vulnerable, inflexible …” Therefore, Stogran concludes that “We should be looking at these technologies to enhance the human network.”

[6] Voice over Internet Protocol (VoIP) is the routing of voice conversations over the Internet or any other IP-based network. See Wikipedia at http://en.wikipedia.org/wiki/Voice_over_IP.

5. The potential for networks to encourage “micromanagement” interference in the chain of command. What style of leadership or command is most appropriate for networked operations?

One specific effect of networks on the chain of command raised, but expressed in different ways, by nearly all of those interviewed was that networks could encourage higher levels of command to micromanage lower levels of command.

Stogran, a tactical-level commander, complained that strategic headquarters interfered in tactical engagements, by demanding so much information and such a high level of certainty that collateral damage would not occur, that operations were sometimes paralyzed and that opportunities to take action were lost. He also believed that strategic-level headquarters had more opportunity to micromanage because CF networks are stovepiped. Devlin gave an example of this type of interference in activities at the tactical level from his current job, as the Canadian Deputy Commanding General US Army III Corps, Fort Hood, Texas, when it became clear during an exercise that one of the division commanders within the corps did not “fully understand what the commander’s concept was and was going off in a direction that was not consistent with what the [corps commander] wanted.” The fidelity of the information on the network allowed corps staff to see the problem quickly and to send staff officers all the way down to division level and even battalion level “telling the division staff it was time for battalion X to adjust its course and you needed to move on this route.” Devlin concluded that this was not an appropriate command style because it violated the principles of mission command and threatened the relationship between commanders, especially the trust and confidence that had been built up to that point. Therefore, he concluded that there has to be a balance between intervening in situations and letting subordinates take the initiative, and that it was important for higher headquarters “to step back and allow the relationships and the mentoring that has taken place and has broadened your force to a certain point, to carry on.”

Natynczyk spoke of the pitfalls of micromanagement at the operational level-strategic level interface. He said that there were people at the strategic level, who, without all the details of a situation, did not understand its nuances or did not see how minor changes could signal major events. Natynczyk said that using technology to show those out of theatre at the strategic level or operational level the context and the significance of what had changed meant that “all of a sudden the lights come on a lot sooner.” For example “doing a VTC at an integrated work station with all of your commanders, you don’t have to restrict [the VTC to] the people in theatre. You can *include* people back at home base in Ottawa to participate in these things. [emphasis in original]” Natynczyk found that this use of technology helped higher headquarters understand when something had changed in theatre, and, therefore either more resources were needed or different technologies were required to adapt to the changing circumstances. He felt that it was particularly important to exploit technology to improve higher headquarters’ situational awareness because, while those in higher headquarters are trying to understand the change, soldiers at the front are facing new threats and could be wounded or killed if their needs were not met in a timely manner. Often higher headquarters’ response to requests were seen as overly bureaucratic by those in theatre, so much so that Natynczyk’s Corps Commander often said: “Bureaucracy *kills*!” [emphasis in original]. And he meant it in a literal sense.

Tabbernor, while expressing concern about the potential for micromanagement, argued that there are circumstances where high level involvement in tactical actions might be warranted:

> The other concern I have with an all-knowing, all-seeing net is the ability of commanders to micromanage and not let people do their job. … Now having said that, there are probably instances where the operation that you are doing at the tactical level will have such a huge impact at the strategic level that let's say a special operations ops somewhere that if it goes wrong, the Prime Minister is going hear about it and the country is going to look like shit. Maybe that's the point in time where the CDS is in fact in the loop.

However, Tabbernor acknowledged that micromanagement could be a problem. For example, when he wanted to move four soldiers from one part of the theatre to another (into Afghanistan) he was told by senior DCDS staff in NDHQ that he could not because, as he was told by one senior staff officer, "…'yesterday we briefed the DM [Deputy Minister] and the DCDS that there were only three people in Afghanistan and if tomorrow we have to tell them there's seven, they are going to want to know why, so you have to send us a briefing note and get approval from the DCDS…'" to move four soldiers from one location to another in theatre. Tabbernor's reaction was: "I never did get the authority. I got pissed off and I just told them to do it anyway." In another instance a senior officer at the strategic level, "was woken up in the middle of the night because …[the Canadian commander in the theatre] needed his authority to move four engineers from Kabul down the road a number of kilometres to help the Americans deal with an issue." The senior officer's reaction was "'Why the hell are you asking me that? I've got a Colonel in theatre who's more than capable of making these decisions.'" These examples show, according to Tabbernor, why "…General Hillier says 'The staff is wagging the dog here.'" Therefore, in Gen Hillier's current CF transformation initiatives the focus is on establishing a command-centric organization to replace the bureaucratic, staff-centred organization that evolved in the 1990s. Tabbernor believes that, organizational issues aside, training remains the best way to ensure that micromanagement remains in check:

> Having been on the receiving end of micromanagement, as a commander, it is not pleasant. I don't know if you can put filters into the system to filter out what individuals should or should not see…in an all-seeing, all-pervasive net. I think it boils down to training. [As a commander] you can see the whole picture, but you can also zoom down onto what the squad is doing. But if you are an operational-level commander, [even if you can] can zoom down to what the squad is doing or the section is doing, that's really not your job. … So I think in a situation like that it is a matter of training so that you force people to push back to where they are supposed to be or where they should be.

Tabbernor concluded that networked operations work best when the commander uses a transformational style of leadership: "You need a leader who can express his intent and then back off and allow his subordinates to do what he's asked them to do, comfortable in his own skin that they will do what he wants them to do." However, he cautioned that he is not suggesting a "delegate and disappear approach," because the commander must monitor subordinates' performance, and intervene when necessary.

In Natynczyk's experience with the US Army, he found that networked systems helped to minimize micromanagement, "because [commanders] don't have to pester subordinate leaders as to what they are doing because they can see it without asking. But at the same time, under mission command, you have to delegate and trust." And Natynczyk saw that trust was improved if superior commanders could see what subordinate commanders were doing at all times without asking, "… It avoids micromanagement. Because the commander can give orders…and then if he wishes, he can sit back and see 'Ah! It's all happening.'" However, Forcier, in describing a joint command experience, said that the Canadian Army was opposed to the type of system described by Natynczyk because they "were afraid…that this would become a tool for NDHQ to get into their business because if it's on the network …[NDHQ would] know. And therefore …[would] interfere." Forcier asserted that the navy and the air force were "used to operating in an environment of information flow," but that the army was not because it was "event driven and to go and push information online, or draw information online is not a natural reaction for them." In his experience as an officer in an NDHQ joint staff, Forcier observed that the Canadian Army resisted installing in theatre the technology to pass classified e-mails back to Canada, and when secure networks were placed in theatre the Army was reluctant to put information like reports and returns, troop dispositions, order of battle, and information about the enemy online.

Devlin expressed the dilemma between delegating and micromanagement in terms of choices that commanders could make in creating their C2 arrangements "… how far do you want to risk not being command-centric and being staff-centric or information-centric? …I think that it is just tied to how much freedom…you want the staff to take and how much freedom the network allows the staff to take." He concluded that there has to be a balance between the two options; however, he noted that "There's a tendency to direct too far down, and it threatens the relationship [between commanders and their subordinates] and threatens the trust and confidence that has been built [between them]." He argued that the best approach for the commander was to step back and allow subordinates to do their tasks based on the relationships that have been established and the mentoring that has taken place.

One way of dealing with the potential growth of micromanagement, according to Gosselin, is a realistic approach to human dimensions of command, especially authority, responsibility, and accountability. He asserted that the central issues to ensure effective networked operations were those of command, decision making, and an individual's ability to tolerate risk. Therefore, Gosselin argued that commanders need to establish their comfort level about the authorities that they possess and about the responsibilities that they have and how their authority and responsibility are related to their accountability. Once commanders understand these dimensions of command, they can use technical networks to execute their missions more quickly.

Some senior naval commanders remarked on significant differences in approaches to command in a networked environment based on systemic cultural biases. For example, Girouard found that the Canadian approach to intelligence is still largely army-oriented, and this resulted in "Reams and reams… of data being pushed at you that really had no pertinence to the work that you were doing…" Because of the Canadian intelligence system's inability to adapt fully to the maritime forces' needs, Lerhe found that it took him a month to get his intelligence officer to understand what his priorities were in theatre.

Natynczyk offered an army perspective on intelligence. He found that when fighting insurgents that it was important to deal quickly with “actionable intelligence.” However, from an army perspective, to ensure precision and to minimize collateral damage in a more complex physical environment than the navy, detailed knowledge of potential targets is required. The only way, in Natynczyk’s view, to act on intelligence in a timely way in counter-insurgency operations is to use technology “to collect the information… [and] turn it around into actionable intelligence to exploit…”, especially if the target is a sensitive one requiring various levels of ratification to engage. But he cautioned that “…the further you are from the sound of the gun, the less you understand. The more you *think* you understand but the less you understand.” Sometimes higher headquarters are influenced by media reports coming out of theatre, “…and the media are focused on the most negative [stories] and where the flash points are. And so no one back home understood what was going on.” He elaborated with this example:

> …in the case of Iraq, we had the Shia and the Sunni uprising around Easter of 2004. In the divisions with the brigade they knew instantly something had changed. … [at] Corps headquarters in Baghdad it took us about a day to understand what happened. To the CENTCOM Staff that was then in Dubai it took about a week to understand. Tampa took a month to understand. Washington…took *two months* to understand! [emphasis in original] Why? Because the further away you get from the theatre, the less and less you deal with issues on the ground. The more you’re dealing with resources [and long term issues].

Some senior commanders noted significant differences in approaches to command in a networked environment based on who was in command. For example, one commander found that one of his superiors constantly requested detailed information, while another superior practiced mission command and gave him “a huge amount of slack.” It is difficult to know what the specific causes of these differences were, but they could be a combination of such factors as personality, education, and experience.

6. The challenge of Canadians conducting networked operations with partners with different technological capabilities.

There are a number of challenges conducting networked operations with partners with different technological capabilities. Tabbernor notes that in his experience in Bosnia there were four nations operating together with very different levels of capabilities, ranging from the Czechs at the low end to the British at the high end of the technological spectrum, with the Dutch and the Canadians in between. A major challenge for those leading these types of operations is to design and to put in place a network that is accessible and understandable to those at both ends of the spectrum. He described Operation Athena (Canada’s contribution to ISAF in Afghanistan) as particularly challenging because the Americans were operating at the very high end of the technological spectrum, while some other coalition partners were “still back in the old days with field message pads and stubby pencils.” Devlin attempted to extend the technical network to coalition partners that did not have the necessary technology by sending Canadian signallers to partners to provide better connectivity to the network than these partners could achieve on their own. Stogran noted that, at the time he was interviewed in early 2006, OGDs did not have networked systems that could match the technical capabilities of CF systems; therefore, human networks were critical to making integrated operations work.

Girouard agreed that technical differences among coalition partners were a problem, and were likely to remain a problem for the foreseeable future. For example, in operations like East Timor and in exercises like RIMPAC, there were technological differences that impacted upon networked operations. The best way to address the challenges posed by these differences, according to this officer, was through effective leadership. He noted that a major challenge for him was ensuring that nations with low-end technical capabilities were still able to get the information they needed to contribute meaningfully to the mission. This could be difficult especially "[b]eing able to deliver that information in a timely fashion without violating the trust" that has been established with those nations with more sophisticated technical networks that give you special source data. This officer emphasized that establishing trust among coalition partners is critical to making the coalition function effectively, but that trust in partners "isn't a miracle that happens"; trust is built by working on relationships and by sorting out various procedures to ensure that all partners have the information they require to do their jobs within the limitations imposed by technology differences and access rules. This process, according to Girouard, involved a "disciplined use of communications" supplemented by liaison visits. Since Canada had access to many secure network sources it was able to give those that did not have full access alternative ways of getting vital information "through aggressive use of battle force e-mail." From a naval perspective, it was not good enough to be in the middle range of technological capability. In order to be Task Force commanders in coalition operations, senior Canadian naval officers required high-end technical capabilities, because, as one of them put it, "if you're not in the know, from a command and control perspective, you become irrelevant."

Devlin agreed that establishing networks in a multinational coalition could be difficult given the access (security) issue. Devlin noted that it was sometimes easier to share resources than information, because information is "one of the most difficult things to share." He added that it was "painful" to see how unwilling some nations were to share information, but that the human network could allow coalition partners to share necessary sensitive information. "It is all about trust…understanding…[and] confidence," he explained. If present, these factors make one nation comfortable about sharing sensitive information with another nation in the coalition.

Natynczyk raised an issue that is sometimes overlooked in networked operations – capabilities can vary among one nation's services and even among units within a service. During his time in Iraq with III Corps, besides the other coalition countries such as the Ukrainians or the Poles, he found that the US Marines "were doing it the old way," and were not as technologically sophisticated as the US Army. He went on to say that even in the US Army there were different levels of technological sophistication in networked operations, and during his time in Iraq the First Cavalry Division was the most sophisticated with "the Divisional Commander using a system called Command Post of the Future." With this system the divisional commander could conduct an evening "collaborative" VTC supported by integrated work stations (IWS) "with every one of his brigade commanders." This gave widely dispersed subordinate commanders the ability to exchange views supported by a digitized representation of the battlespace on their IWS, and "based upon what he was seeing, the division commander could update his intent…[and] his direction immediately." Natynczyk described this process as "…totally network enabled. And yet the personal touch was there."

Virtually everyone interviewed for this project agreed that, given the operational necessity of working within coalitions and alliance arrangements where not everyone will possess the same degree of technological sophistication, networked operations require a combination of both technical systems and personal relationships.

7. Competencies required by senior commanders to manage both the technical and the human dimensions of network-enabled systems

In order to successfully use networked systems, those interviewed felt that commanders must have an awareness of both the technical and the human dimensions of network-enabled systems. Devlin underscored this point: "… balancing what is available from a technological point of view with what we do on the people side is vital. If we don't have that balance we will screw things up."

Natynczyk emphasized the importance of training and experience in preparing senior commanders to work with network-enabled systems:

> You do not understand this stuff reading a book. You do not understand this stuff studying. You do this stuff with a head set, with plasma boards in front of you, with all of the injects coming together; the fusion happens inside your brain especially after a while where you're able to disseminate this information, fuse it together and see the battlefield, and develop a level of intuition. Then take that headset off, get in a vehicle, get on the road, fly, go on the ground and see it. Talk to people. Understand their conditions and the realities of battle. Come back into your headquarters with this knowledge and now you take it to the next level. [Also encourage] your staff to get out on the ground to see what you saw, but now your ability to make effective decisions is incredibly enhanced. And that saves lives.

Gosselin believed that commanders had to understand enough of the technical dimensions of network-enabled systems to be able to properly specify their requirements. In other words, by understanding the limitations of technology, commanders can state their needs within the bounds of technology. This understanding also allows commanders to ask the right questions when framing their requirements. Therefore, Gosselin felt strongly that commanders must have the same degree of technical understanding of their network technology as they do of any other major combat system so that they can specify their requirements in operational terms. Once commanders have defined their needs in operational terms, e.g., secure access to all liaison officers, it is the job of the technical experts to meet those needs. Unfortunately, according to Gosselin, the CF tends to take the reverse approach, whereby technical specialists are asked by commanders what they can provide in the way of capabilities and then commanders select from the menu of capabilities provided by the specialists. Gosselin blames senior leaders for this state of affairs because commanders and senior staff often cannot articulate their C2 needs adequately. He concluded that: "If you don't understand what it [technology] can do for you, if you don't take the time to ask the questions, then you're not helping. It's like if you don't understand the capability of your combat system…"

Natynczyk implied that the Canadian Army did not understand enough of the technical dimensions of network-enabled systems to succeed in its transformation because, in his view, the technological aspect of Canadian Army transformation “to be quite frank has been a dismal failure” due to the kind of technology that was bought. The equipment that was bought has not given the Army the effect that it desires, he continued. Whereas, the Canadian Navy is “much better off because they have an imperative to be interoperable with the US Navy,” and, he suggested, that the Canadian Air Force has essentially the same interoperability needs as the Canadian Navy because of the Air Force’s close integration with the US Air Force in such organizations as NORAD.

An example of understanding the technical dimensions of networks from a naval perspective was provide by Lerhe who said that the commander must understand his communications systems sufficiently to appreciate the allocation of bandwidth capacity to his subordinate departments, because bandwidth out of theatre is always in short supply. Therefore, a technically aware commander will alter bandwidth allocation as he moves from the operational theatre (at sea) to port and vice versa. More specifically, this officer felt that a task force commander must understand that there are typically four demands on communications band width. There are 1) the intelligence load, mostly information coming in and not much going out; 2) the command and control load, the commander directing other forces, mostly information going out; 3) the flagship load which is often combined with task force logistics; 4) and then the personnel and administration load. The commander must know how to adjust the bandwidth ratio allocated to each load, because depending on the circumstances each load requires a different allocation of scarce bandwidth for the operation to be conducted effectively.

This same naval officer felt that the Canadian Navy’s practice of having operational (MARS) officers remain in charge of the procurement and application of communications technology was superior to the Army and Air Force practice of allowing technical specialists to effectively take over the design and procurement of communications systems. He argued that by turning responsibility for communications systems over to technical specialists, Army and Air Force officers had lost awareness of technological constraints that this awareness is essential to operate effectively in a network-enabled environment.

Along similar lines, Girouard expressed a sense of unease with the growing centralization of the control of communications technology in the CF, and, therefore the potential loss of influence by the operational chain of command on shaping that technology. He believed that in some cases, technical experts exert too much control on the content that is added to the network. This trend was particularly worrisome to him in the context of the creation of networked systems and who decides which person gets what information. Too often he found that the technical experts’ desire to keep a close hold on information was overriding operational requirements. He put the dilemma this way, “Is the distribution of information about timeliness and effectiveness in keeping folks safe, or is it about security and keeping…controls as a default? … I think a one size fits all answer to that [question] is inappropriate. … But I don’t think that systemically we’ve sat down and had this conversation. … I think there’s a growing tendency to centralization as I see things like the IM [Information Management] Group taking the comms and that concerns me. I think that runs counter to effectiveness of the operation philosophically.”

Tabbernor found that when there were problems with technical systems in the field, that it was the ability of humans to adapt the technical systems to overcome situations that could not be predicted by designers of technical systems that was critical. Girouard agreed that human capabilities to adapt technical systems were critical to meeting the operational need. Therefore, he expressed concern that centralization of decision making on technical systems was hampering the ability of humans to make adaptations to technology to meet the requirements of commanders conducting operations.

Girouard noted that there has been significant progress in the connectivity, timeliness, rapidity of information transfer, and fidelity of networked systems. However, in his opinion, the challenge today is to present the commander with a manageable amount of information by sorting the relevant from the irrelevant. A combination of technological awareness and an awareness of the human dimension of command is required by commanders to discriminate between useful and irrelevant information provided by the network according to Girouard . He did not think that either technical systems or those running them should be responsible for determining the value of information; he believed that the intelligence community and the operators had that responsibility. However, he did not believe that they were always as effective as they should be in discharging that responsibility, and that sometimes technical concerns were allowed to take precedence over operational imperatives. He concluded that getting “the right stuff at the right time to the right guy in need” is the “holy grail” of networked operations today. One way to approach this ideal is to take better advantage of the competencies of all of those, including NCMs, who are nodes in the network, and to encourage them to be disciplined and to provide commanders with the information that commanders need based on their understanding of commander’s intent. He elaborated on this idea by saying that individuals needed the competencies to understand where they fit into both the human and the technical networks, and, based on commander’s intent, take the initiative to select what information they need to focus on among the mass of data available and then make judgements about when to engage superiors with relevant information.

Another dimension of this issue, according to Gosselin, is the CF’s culture. One aspect of CF culture that impedes the ability of some commanders to fully exploit the potential of a networked environment is a military culture that is geared towards secrecy, where sensitive information is kept within a small circle of “need to know” individuals, he argued. Gosselin contrasted this with the Foreign Affairs approach where sensitive information is disseminated much more quickly to a larger group of people. As he sees it, this tendency to restrict the dissemination of too much sensitive information negates the value of networked operations, because without access to this information the system will not work properly.

Another aspect of CF culture that interferes with the ability of some commanders to fully benefit from the potential of a networked environment is the belief, by some, that commanders need to see all the information possible, rather than letting their staff filter the information for them. Sometimes this situation arises from a lack of technical understanding of networked systems, as described above, and sometimes it arises because of a culture of micromanagement where some CF commanders are not able to practice mission command effectively. If commanders are not clear in their own minds what information they need to see to practise mission command, Gosselin declared that “the temptation is to say give it all to me. I’m not too sure, but give it all to me. … I think it's critical that [commanders] just don't get…all [the information]. … commanders [should] state what they need and let the staff do the sorting and the analysis…Most commanders… won't take the time to…really state their requirements and without doing that, you get everything." He concluded that with the sheer quantity of information available in a networked environment commanders had to develop the ability to "be comfortable in not seeing everything and knowing everything."

8. Personal lessons learned from working in a networked environment.

For Tabbernor, the most significant personal lesson learned from his experience working in a networked environment was that, in the end, "command is a face-to-face matter," and that at some point commanders needed to spend time with their subordinates to establish common intent and trust.

Another way of establishing common intent and trust employed by almost all of those interviewed was the use of liaison officers to meet with coalition partners personally and to thereby supplement the technical network. Stogran believed that, by using a human network of liaison officers in Afghanistan, he was more informed on some issues than the American general he worked for who did not use liaison officers as effectively. Similarly, Gosselin said that the most important lesson that he learned working in a networked environment was the importance of placing sufficient numbers of liaison officers at sufficiently high rank levels in as many locations as possible. Although this practice is often resisted by those who build hierarchical organizations, Gosselin advised putting liaison officers "everywhere" to help build situational awareness. He believed that the personal interpretation and context that liaison officers could provide was critical to making informed decisions.

Another important issue for working in networked operations, according to Gosselin, is the necessity to improve the willingness of senior leaders to delegate decision making authority. He believes that while accountability remains with commanders, delegation of authority must be practised more frequently: "…you need to ask yourself very clearly; why do I have to make that decision? And [the reason given] should not be because the one before me did it."

Devlin believed that Canada needed to continue to pursue the tremendous potential resident in networks: "we shouldn't wait for others to develop it, we should develop it with them… [or] we will end up being the ones left behind." If the potential is realized it will enable Canadian commanders "to be faster, to give better decisions, to have greater insight, and to have a force that is better protected and better equipped to be able to undertake the difficult missions that any nation asks their solders to do."

Natynczyk suggested that one way to develop a networked capability in Canada relatively quickly and to mitigate the risk of acquiring new technology is to buy proven, interoperable products that are user friendly because "we don't have enough money to invest in leading edge technology." Once the equipment is acquired it is essential to educate and train everyone from private all the way up to general officer how to use the technology.

Based on his experience with the US Army's III Corps, in garrison, in Korea and in the Middle East, Natynczyk found that "network enabling technologies allow commanders at all levels from section…up to corps to be able to see the battlefield … [to] assist in [their] decision making, [and to] allow them to figure out where to focus. And when they did focus they ventured out on the ground to talk to divisional commanders, brigade commanders, battalion commanders, and below." Given the size of a theatre like Iraq, it was impossible for the corps commander to be everywhere; therefore, it was important for him to know where it was critical "to go out on the ground to see the problems, talk to the leaders" face-to-face, to give them amplifying direction, and to put their specific operation into a broader context. Getting out to speak to commanders other than the ones involved in the main effort also allowed the corps commander to help all the adjoining divisional, brigade and battalion commanders to understand where the main effort was and to understand what their contribution to that main effort was compared to their own missions. Supplementing these face-to-face meetings was a technological network that facilitated commanders getting their update on the situation first thing in the morning – "we called it battlefield circulation. Walking the ground, talking to folks, and then [the higher-level commanders] recovering back to [their headquarters] to provide orders to their staff. Battlefield circulation allowed "commanders come back to empower the staff with updated information knowledge and context," and this helped commanders to modify their commander's intent and to issue the orders to enable that intent. "This balance between…technological enablers and…human interaction…is essential," he concluded.

Natynczyk also commented on cultural aspects of Canada's use of networked operations in coalitions: "I think we have a culture in the community and the military, perhaps in Canadian society [of being]…self depreciating. Where we continue to demonstrate this lack of confidence in ourselves. And yet every time we send troops into whatever theatre or situation, be it domestically at home…we come out recognizing that we are the best, if not among the best of services in the *world*! [emphasis in original]" One of the reasons for the proficiency of Canadian military personnel is the personal qualities of junior leaders in the CF. To maintain this proficiency Natynczyk argued that "…the key [is] focusing on junior leaders [to] ensure that they have cohesion, the knowledge, but very importantly the confidence that they be trained to high standards have a self-discipline and are physically fit." He went on to say, "…I would put them man for man, woman for woman, unit for unit against any comparable organization or individual from any other country in the world within our competency…because we have high standards. And whatever service we have, our culture is to set very high standards. And we hold people to those standards. We fail people if they don't measure up to those standards. And we tell them to take a new direction. We have incredible discipline. It's a factor of our culture and our heritage. And as a result of those two combinations, we can put people into harm's way, and with the knowledge that they have, they can be flexible to adapt their knowledge to the new circumstances on the ground."

CONCLUSIONS

In order to fully understand the nature of NEOps today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to document recent Canadian experiences with networked operations. This report addresses these issues based on an analysis of interviews conducted during Jan and Feb 2006 with eight Canadian commanders who had recent experience with networked operations at the operational level of command. A summary of the key points raised in the interviews follow by topic.

Different interpretations of the meaning of terms associated with networked operations. There was consensus among those interviewed that there are many different interpretations of terms associated with networked operations. However, there was no consensus on the precise meanings of these terms. Those who gave detailed comments on this issue felt that part of the reason for a lack of consensus was that the concept of networked operations was being influenced by many different stakeholders. A number of those interviewed observed that concept development of networked operations was too often driven by technical requirements rather than user requirements. All those interviewed agreed that networked operations were going to be an important part of future military missions; therefore, they recognized the need to work towards a common understanding of what networked operations means in different contexts.

Differences in how networked systems are used. One of the problems with achieving a common understanding of networked operations is that there is no standard model for a networked system, because different missions and different operating environments require different types of networks.

Despite the differences in networked systems, almost all of those interviewed commented on the need to establish trust among those working in an operation through face-to-face contact. While technical systems like VTC could facilitate establishing trust, personal contact was seen as necessary to build common intent and to minimize misunderstandings. A commander who had worked with the latest US Army networked systems said that a major advantage of their systems was that they gave the senior commander the capability to pick out from a very complex picture those few indicators that could spell the difference between success and failure and to focus on them. Furthermore, the technical system could give commanders information to help them decide where to intervene personally. Many felt that it was important to have personal contact early in an operation to lay the foundations for establishing trust and common intent and that, wherever possible, teams should be composed of people who have worked together with each other and with the commander.

The effect of networks on command. Those interviewed had differing views on how the use of networks affected how command was exercised in operations. For one, the negative effects on the chain of command of the distance between the Canadian operational-level headquarters and the theatre of operations could only be partially mitigated by technical networks. Sometimes information available on the network could help to overcome the lack of personal contact among members of the human network, for example, a commander's intent could be enhanced by the technical network if it had been well articulated and well understood in the first place through the human network. Other commanders found that the volume of other information on the network interfered with the ability of commanders to articulate their intent over the “noise,” like “chat,” on the network. In other cases, some commanders found the widespread availability of information on the network could also undermine the authority of the chain of command, if operational commanders were unaware of information that affected their subordinates and if the commanders had not been advised of this information or consulted about policy changes.

In summary, most of those interviewed believed that human networks created through human relationships are critical to effective operations and, while technical networks are essential to support the human networks, the technical networks must be used in such a way that they enable rather than detract from the exercise of command.

The need for both human networks and technological networks, and the relative value of each. All of those interviewed recognized that both human networks and technological networks were required in today’s operations. Likewise, they agreed that the technical network should enable the human network. However, how the technical network could enable the human network will vary according to circumstances. Those who have worked in relatively homogeneous organizations, like the US Army, where the technical and human systems appear to be relatively well integrated and supported by common doctrine and extensive training, have a great deal of confidence in the technical systems. Those who have worked in heterogeneous organizations, composed of military forces of various nationalities and sometimes composed of civilian organizations, have relied more on human systems than technical systems. In fact these commanders found that one of the key functions of the human system is to find ways to compensate for technical, doctrinal and training disparities among members of these organizations.

The potential for networks to encourage “micromanagement” interference in the chain of command. What style of leadership or command is most appropriate for networked operations? One specific effect of networks on the chain of command raised by all those interviewed, but expressed in different ways, was that networks could encourage higher levels of command to micromanage lower levels of command.

In general terms, lower levels of command perceived that, at least some of the time, higher levels of command were interfering inappropriately in their activities. Those at lower levels of command observed that higher headquarters did not routinely practise mission command, the preferred doctrinal leadership/command philosophy espoused by the CF. They also complained that higher headquarters often acted in a bureaucratic manner that met the needs of the staffs of higher headquarters, but did not necessarily meet the needs of those engaged in operations. Those at lower levels of command also complained that higher headquarters interfered too much in tactical details and burdened subordinate commanders with requests for large amounts of, what seemed to the lower command levels, to be irrelevant information. On the other hand, most agreed that when tactical actions could have a major impact at the strategic level, close oversight from higher headquarters was warranted.

While many found that the increasing use of technical networks was facilitating micromanagement, those with experience in highly sophisticated US Army networks found that, if properly trained, commanders could resist the temptation to interfere inappropriately because the information provided by the technical network enabled them to monitor subordinates' action to ensure that commander's intent was being realized.

Virtually all of those interviewed agreed that mission command was the preferred command philosophy for networked operations; however, many observed that environmental (or service), cultural and individual differences in interpreting how that philosophy should be applied in practice caused problems in networked operations.

One way of dealing with the potential growth of micromanagement in networked operations is to understand the relationships among a commander's authority, responsibility, and accountability. Therefore, to be as effective as possible, commanders should examine these relationships early in their tenure and establish their own comfort level with them. Most agreed that education, training and proper procedures were the best way to ensure that micromanagement remained in check.

The challenge of Canadians conducting networked operations with partners with different technological capabilities. The challenges of conducting networked operations with partners, including OGDs and NGOs, with different technological capabilities are unlikely to change significantly in the foreseeable future. It was also noted that there were significant differences in the technological networks used among the US services, and even within a service, depending on the degree to which a particular unit had been equipped and trained to operate in a networked environment. In large coalitions there will always be technological gaps to bridge. In addition, any time the CF works with the US armed forces, except in specific circumstances like NORAD where technological compatibility is the norm, there will be issues of technological interoperability to resolve. Many of those interviewed found that the best way to bridge technological gaps was by using human networks. However, the success of human networks in bridging these gaps depended to a large extent on effective leadership. And a key role of effective leaders was to establish trust among coalition partners by working on relationships and by sorting out various procedures to ensure that all partners have the information they require to carry out their missions, given the limitations of technology differences and access rules. A major obstacle to building the necessary human networks was the unwillingness of some nations to share sensitive information; however, this problem could be mitigated by actively building trust, understanding, and confidence among coalition partners. Given the nature of future coalition operations where partners are likely to have widely varying network capabilities, human networks will be required to bridge the technological gaps.

In developing concepts for networked operations in this country it should be clear that "one size does not fit all," because the needs for sophisticated technical networks among the environments in the CF can vary almost as much as the needs among coalition partners, according to those interviewed. For example, while the Canadian Army can utilize technical networks in the mid-range of complexity for most of its operations, the Navy and the Air Force, because of their close integration with US forces, require high-end technical capabilities to be interoperable in the maritime and aerospace realms, especially if Canadians wish to exercise operational command.

Competencies required by senior commanders to manage both the technical and the human dimensions of network-enabled systems. Commanders must have an awareness of both the technical and the human dimensions of network-enabled systems in order to effectively command in a networked environment, according to those interviewed. Those with the most experience working with highly sophisticated US systems were adamant that training and handson experience were essential to using the technical network effectively, but that even with these sophisticated systems it was critical for commanders to supplement the information given to them by the technical network with information acquired “on the ground.”

An important competency, lacking in some of the CF’s senior officers, is an understanding of enough of the technical dimensions of network-enabled systems to be able to properly specify the commander’s information requirements, notably in terms of the outputs required by the commander. Some felt that the approach to networks taken by the CF was not as effective as it could be, especially in cases where commanders and senior staff could not adequately articulate their C2 needs, because they then accepted technical systems designed by specialists that, while technically sophisticated, did not meet their C2 needs. The Canadian Army was singled out by some of those interviewed as particularly representative of this type of problem. Another reason for this problem, according to Girouard and Lerhe, was the loss of influence of the operational chain of command on shaping network technology. This, they believed, had occurred because of the growing centralization of the control of communications technology in the CF, resulting in too much influence by technical experts on the content of the network.

Problems that some Canadian commanders have had working in a networked environment are exacerbated by a culture of micromanagement in some parts of the CF that encourages senior officers to try to see too much information rather than letting their staff process the information for them. Another facet of CF culture that impedes the effective use of networked systems by some senior officers is a military culture that prizes secrecy above sharing of information. It appears that some senior officers use “information power” to fuel a culture of micromanagement rather than practise mission command.

These concerns notwithstanding, most of those interviewed felt that humans had the ability to overcome most of the problems described in this section. But to overcome these problems, those working with networked systems need the competencies to understand where they fit into both the human and the technical networks, and then they need to have leaders who will let them use their initiative to meet the challenges of working in a networked environment.

Personal lessons learned from working in a networked environment. A number of those interviewed articulated what they felt were some of the most important lessons that they learned from working in a networked environment. Many concurred with the statement that “command is a face-to-face matter,” and that to establish common intent and trust commanders needed to spend time getting to know their subordinates, preferably before a deployment or mission. Establishing common intent and trust among coalition partners could not always be accomplished before a mission; therefore, almost all of those interviewed employed liaison officers to meet with coalition partners to build common intent and trust. It was found that the personal interpretation and context that liaison officers could provide to commanders was critical to their ability to make informed decisions.

A challenge for Canada will be to develop a networked capability relatively quickly because traditional procurement cycles cannot keep up with the rate of technological change. Given the CF’s budgetary constraints, one of those interviewed suggested that the best way to mitigate the risk of acquiring new network technology is to buy proven, interoperable products that are user friendly. He added that any procurement strategy must include a rigorous training and education program to prepare all those who will use the system in all aspects of its use.

All those interviewed had different experiences working in a networked environment depending on the sophistication of the network and the circumstances in which the network was employed. Some relied heavily on human networks to overcome problems with technical networks. Those with experience in highly effective and sophisticated networks relied more heavily on technical networks than those who did not. However, given the unpredictable nature of future operations, especially the unpredictability of the nature of future partners, whether they be military, paramilitary or civilian, both human and technical networks will be critical to success in the networked environment of the future.

Canada has a number of advantages in this unpredictable environment. Even though some believe that Canadian culture promotes a self-deprecating attitude that could be interpreted as a lack of confidence by some, Canada’s military culture provides the foundation for extremely effective armed forces. Some of the factors that contribute to that effectiveness are the personal qualities of junior leaders in the CF, high professional standards, discipline, and the ability of CF members to adapt to changing conditions. Even so, some of those interviewed felt that it was possible to do more to maximize the potential of all of those working in a networked environment through improved education, training and experience.

A challenge for the CF today, raised by one of those interviewed, was how to articulate the concept of networked enabled operations as the CF transforms from a staff-centric or bureaucratic philosophy to a command-centric philosophy. A key part of that challenge will be achieving a balance between the requirement for standardized systems and procedures and the need to customize network products to meet each commander’s unique requirements.

This page intentionally left blank

ANNEXES

Drdc Human Research Ethics Committee Submission

Submitted 26 October 2005

Protocol Number: L535

Title: Canadian Experiences with Network Enabled Operations

Short Title: NEOps - Canadian Experiences

Principal Investigator: Dr Allan English, KMG Associates, Kingston ON (under contract to DRDC Toronto).

Co-Investigators: Dr Richard Gimblett, KMG Associates
Mr Howard Coombs, KMG Associates
BGen (retired) Joe Sharpe, KMG Associates
Mr Keith Stewart, DRDC Toronto

Thrust: 16kj

Background:
The concept of Network Enabled Operations (NEOps) is central to the Transformation of the CF that is now being undertaken. The NEOps concept is being developed to support the specific range of capabilities that the CF will need to be able to field in future to meet Canada's strategic aims. The concept is not developing in a vacuum however. Similar concepts have been maturing in partner nations over the past decade. For example, the US concept of Network Centric Warfare is conceived as 'a combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage'. More recently, the United Kingdom Ministry of Defence has developed its own concept of Network Enabled Capability and other nations, notably Australia and Sweden, are working on their own network-based approaches to operations. It is significant that while these concepts are all based upon the idea that operational advantage can be gained through the harnessing of network technology, there are subtle differences within each nation. For example, NCW in the US is aimed primarily at warfighting and has traditionally focused on the Department of Defence. The UK takes a wider view and recognizes the potential for NEC to support capability across a broad spectrum of operations. Moreover, by emphasizing a 'commander-centric' view of net-based operations, the UK has resisted the implication that net-based operations are necessarily network-centric. Likewise, Canada's concept of NEOps needs to develop to meet the requirements of the CF, for example in implementing the 3D (Defence, Development, and Diplomacy) approach advocated by the Government. This study will contribute to a clearer definition of the NEOps concept. This

concept is emerging through discussions and papers within DRDC and jointly with other players in the Department. A particular concern of DRDC Toronto in this regard is the human factors (HF) implications of the concept, the critical HF issues and the establishment of a research agenda to address them.

To date very little has been written on the Canadian experience with Network Enabled Operations, particularly at the operational level of command. A recent DRDC Contract Report, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," noted that Canada has made significant contributions to the evolution of networked operations, but that these contributions have not been well documented. In order to fully understand the nature of Network Enabled Operations today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to document recent Canadian experiences with networked operations.

Purpose of the Study:
The purpose of the study is to interview selected senior Canadian commanders about their experiences in networked operations and to prepare a paper based on these interviews that documents recent Canadian experiences with networked operations. The paper will provide a context for the experience of these commanders, compare the nature of networking in the various contexts, outline both positive and negative aspects of networking and provide conclusions about how these experiences have contributed to the emerging theory of Networked Enabled Operations in the CF.

Selection of Participants:
The study participants will be senior Canadian commanders with recent experience with networked operations. 8 officers with the equivalent rank of Col, or higher, will be invited to contribute to the study. Potential participants will be selected, in consultation with the DRDC Scientific Authority, on the basis of their knowledge of and experience with networked operations at senior command levels. Apart from experience, there are no barriers to participation in this study. Participants will be under no obligation to take part. Moreover, they will have the option of withdrawing from the study at any stage.

Methodology and Data Analysis:
Prior to their participation, potential participants will receive an Information Letter describing the study (see Annex A). If they agree to participate, participants will sign an informed Voluntary Consent Form at the time of the interview (see Annex B). Participants will also have an opportunity to view the interview questions prior to their participation (see Annex C, Interview Guide). Interview questions will focus on their knowledge of and experience with networked operations at senior command levels.

Before the interview begins, participants will be briefed on the objectives of the study, its relevance and potential benefit to the military, the nature of their participation (i.e., format of interview, time commitment), and associated risks. It will be emphasized to participants that their responses during the study will be kept strictly confidential; that the content of their interview will not be available or accessible to supervisors, peers or subordinates; that if excerpts from interviews are to be used in reports or publications, under no circumstances will their identity be reported without their express written consent. It will be made clear to those who are invited to be interviewed that their participation must be entirely voluntary and that their participation (or nonparticipation) will in no way impact their career. Potential participants will also be provided an opportunity to seek clarification or further information from the Principal Investigator before, during, or after the study.

Semi-structured interviews will be conducted at locations convenient to the participants between November 2005 and February 2006. The interview protocol will be designed to allow participants to present the issues that they believe are relevant to their experience as senior Canadian commanders with recent experience in networked operations as well as to provide a common framework across interviews. The questions in the Interview Guide (see Annex C) are based on issues identified in “Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation.” It is expected that approximately eight personal, one-on-one interviews will be conducted. All interviews will be conducted by the Principal Investigator or one of the Co-Investigators. Each interview is expected to last 1-2 hours. Participants will be interviewed only once. Interviews will be tape-recorded with consent, and subsequently transcribed verbatim.

In addition, participants will be sent a copy of their interview transcript for verification. At this time, participants will have the opportunity to indicate any errors in transcription/content as well as any portions of the transcript that they would not like referred to in any reports or publications of the findings. (This may include the entire interview transcript, even if they initially agreed, in principle, to allow the Principal Investigator to quote directly from the interview without attribution of identity, on the Voluntary Consent Form; see Annex B.) When the participants have each had an opportunity to review their own transcript, the investigation team will conduct analysis of the interview content. The purpose of this analysis will be to derive common themes raised by the interviewees and to identify areas of agreement and disagreement relating to those themes. In addition, significant issues raised by a subset of the participants will be captured, for example, where these pertain to particular environmental or operational circumstances. After the completion of the study, a summary of the research findings will be provided to all participants.

Physician Coverage and Medical Screening
Owing to the nature of the study medical screening and physician coverage are deemed unnecessary.

Risks and Safety Recommendations:
Participants will be asked questions about aspects of their work lives and leadership issues that may arouse some psychological discomfort. To offset this possibility, it will be emphasized in the Information Letter that participation in this research is entirely voluntary, that participants may withdraw from the study at any time without penalty, that participants' responses will remain anonymous and confidential, that the content of their interviews/all research data will not be made available to supervisors, peers or subordinates, and that they will receive a copy of the findings once the study is complete. Participants will be told that they may refuse to answer any questions or withdraw their participation at any time. Interview participants will be sent a copy of their interview transcript for verification, at which time they may indicate any portions of the transcript that should not be referred to in any reports or publications. This may include the

entire transcript. They will also be informed that the direct quoting from interviews will only be done with their consent. Participants will also be invited to contact the Principal Investigator if they have any questions or concerns related to their participation. No incentives for participation, remuneration or compensation will be used. Participants will be informed, in the Information Letter and Voluntary Consent Form, that their identity will be completely protected in that only the Principal Investigator and Co-Investigators will have access to the interview or study data. After the research project has been completed, the raw data will be destroyed unless participants indicate on the Voluntary Consent Form that the Principal Investigator may retain their raw data. If participants do not consent to the Principal Investigator retaining their raw data, those data will be destroyed no later than 8 months after the date of the interview. If participants withdraw from the study, their data will be destroyed.

Benefits of Study:

This research will benefit the CF in that it will contribute to a better understanding of the concept of Network Enabled Operations (NEOps), which is central to the Transformation of the CF that is now being undertaken, particularly HF implications of the concept and a research agenda to address those implications. Information from this study may contribute to improving certain aspects of CF Transformation. These benefits outweigh any potential risks, particularly as participants will be informed that their participation is entirely voluntary, that they can withdraw from the study at any time without penalty, that they can refuse to answer any questions, and that their identity will be protected unless they give their written permission to disclose it.

References:

Babcock, Sandy. “Canadian Network Enabled Operations Initiatives.” Ottawa: National Defence Headquarters [NDHQ], Directorate of Defence Analysis [nd, 2004?].

Barnett, Thomas P. “The Seven Deadly Sins of Network-Centric Warfare.” *US Naval Institute Proceedings* 125, no. 1 (January 1999), 36-9.

Cebrowski, Arthur K. and John J. Garstka. “Network-Centric warfare: Its Origin and Future.” *US Naval Institute Proceedings* 124, no. 1 (January 1998), 28-35.

English, Allan Richard Gimblett, and Howard Coombs, “Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation,” report written for Defence Research and Development(DRDC)- Toronto, July 2005.

Free, Jennifer. “Network-Centric Leadership: Why Trust is Essential.” *US Naval Institute Proceedings* 131, no. 6 (June 2005), 58-60.

Gimblett, Richard. *Operation Apollo: The Golden Age of the Canadian Navy in the War Against Terrorism*. Ottawa: Magic Light, 2004.

Johnson, Chris. “Net-centric Fogs Accountability,” *US Naval Institute Proceedings* 129, no. 5 (May 2003), 32-5.

Mitchell, Paul T. “Small Navies and Network-centric Warfare: Is There a Role?” *Naval War College Review* 56, no. 2 (Spring 2003), 83-99.

Thomson, Michael H. and Barbara D. Adams, “Network Enabled Operations: A Canadian Perspective,” DRDC - Toronto contract report CR-2005-162, 13 May 2005.

US Department of Defence, Office of Force Transformation. *The Implementation of Network-Centric Warfare* (5 January 2005), 3. Available at http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf.

Annex A:
Information Letter:
Canadian Experiences with Network Enabled Operations

Dear Participant:

My name is Dr Allan English and I am a researcher at KMG Associates in Kingston ON. I am conducting a study, under contract to DRDC Toronto, with my colleagues Dr Richard Gimblett (KMG), Mr Howard Coombs (KMG), BGen (retired) Joe Sharpe (KMG), and Mr Keith Stewart (DRDC) entitled "Canadian Experiences with Networked Enabled Operations." I should be most grateful if you would assist me with this study by agreeing to participate in a one-on-one interview. This project has been approved by the Defence R&D Canada Human Research Ethics Committee (DRDC HREC). The relevant Protocol Number is L535. I would like to provide you with more information about this project and what your involvement would entail, should you choose to participate.

The concept of Network Enabled Operations (NEOps) is central to the Transformation of the CF that is now being undertaken. However, to date, very little has been written on the Canadian experience with Network Enabled Operations, particularly at the operational level of command. A recent DRDC Contract Report, "Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation," noted that Canada has made significant contributions to the evolution of networked operations, but that these contributions have not been well documented. In order to fully understand the nature of Network Enabled Operations today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to document recent Canadian experiences with networked operations. The purpose of the study is to interview selected senior Canadian commanders about their experiences in networked operations and to prepare a paper based on these interviews that documents recent Canadian experiences with networked operations.

Your participation in this study is completely voluntary. It will involve participating in a single one-on-one personal interview to discuss issues related to recent Canadian experiences with networked operations. The interview will be approximately 1-2 hours in duration and will follow a semi-structured format. The proposed question list is appended to this letter. It is stressed that this list is unlikely to be exhaustive and you are encouraged to raise issues not covered by these questions where you believe them to be relevant to the investigation. If you agree to be interviewed, you will be contacted to arrange a time and place for the interview.

The information that you provide in the interview is considered completely confidential. The interview will be recorded and transcribed, with your consent, and only researchers associated with this project will have access to it. The content of your interview will not be made available or accessible to supervisors, peers or subordinates. After your interview has been transcribed, you will have the opportunity to review its contents (point out any errors, etc.) and to indicate any portions that you would like not be referred to in any reports, publications or presentations (this may include the entire transcript). Review of the interview transcript is likely to take a further hour of your time.

The risks associated with your participation in this study are minimal (i.e., the possibility of harm or discomfort is anticipated to be no greater than what you will encounter in your daily life or occupation). However, participation in this research will involve discussing aspects of your work life that you may find uncomfortable. To offset this risk, you may decline to answer any questions, and you may terminate your participation at any time, without penalty. There are no other known or anticipated risks to you as a participant in this study.

On completion of this study, a research report will be provided to you, submitted to a variety of journals and presented to conferences.

If after reading this letter you have any questions regarding this study or would like additional information, please feel free to contact Dr. Allan English at 613-544-5294 or at kmg1@sympatico.ca. Thank you in advance for your interest in this project. It is greatly appreciated.

Yours sincerely,

Allan English, PhD
KMG Associates

Annex B:

Voluntary Consent Form

Protocol Number: L535

Research Project Title: Canadian Experiences with Network Enabled Operations

Principal Investigator: Dr. Allan English

Co-Investigators: Dr Richard Gimblett, KMG Associates
Mr Howard Coombs, KMG Associates
BGen (retired) Joe Sharpe, KMG Associates
Mr Keith Stewart, DRDC Toronto

I, ______________________ (name) of ___________________________________ (address and phone number) hereby volunteer to participate as a subject in the study, Canadian Experiences with Network Enabled Operations (Protocol L535).

For Subject Enquiry: I have read the information letter, and have had the opportunity to ask questions of the Investigator. All of my questions concerning this study have been fully answered to my satisfaction. However, should I have any questions or concerns regarding this project before, during, or after participation, I understand that I am encouraged to contact Defence R&D Canada Toronto (DRDC Toronto), P.O. Box 2000, 1133 Sheppard Avenue West, Toronto, Ontario M3M 3B9. This contact can be made by surface mail at this address or in person, by phone or e-mail, to any of the numbers and addresses listed below:

* Principal Investigator: Dr. Allan English, 613-544-5294 or at kmg1@sympatico.ca.
* Chair, DRDC Human Research Ethics Committee (HREC): Dr. Jack Landolt, 416-635-2120, jack.landolt@ drdc-rddc.gc.ca.

I understand that I will be given a copy of this consent form so that I may contact any of the above-mentioned individuals at some time in the future should that be required.

I have been told that I will be asked to participate in a single one-on-one personal interview lasting 1-2 hours.

I have been told that there is one risk associated with this research. The risk is that this research will involve discussing aspects of my work life that I may find uncomfortable. To offset this risk, I may decline to answer any questions, and I may terminate my participation at any time, without penalty. There are no other known or anticipated risks to me as a participant in this study.

<u>For Canadian Forces (CF) members only:</u> I understand that I am considered to be on duty for disciplinary, administrative and Pension Act purposes during my participation in this study. This

duty status has no effect on my rights to withdraw from the study at any time I wish and I understand that no action will be taken against me for exercising this right.

I understand that I am free to refuse to participate and may withdraw my consent without prejudice or hard feelings at any time. Should I withdraw my consent, my participation as a subject will cease immediately. In this case, I will have the option of requiring that any data that I have provided be destroyed. I also understand that the Investigator(s), or their designate, may terminate my participation at any time, regardless of my wishes.

Volunteer's Name _________________________
Signature: _________________________
Date: _________________________

I grant permission to have my interview <u>tape-recorded</u>.

Participant's signature______________________________________ Date __________________

I have been advised that, except where I grant permission for direct quotations to be used, all data concerning my participation in this study, including the information that I provide during the interview, will be treated as confidential, and not made available in raw form to anyone other than the KMG Associates and DRDC - Toronto Investigator(s).

I have been informed that I will have the opportunity to review my interview transcript before any analysis is conducted. At that time – even if I have already granted permission to quote from the interview by signing this letter – I will have the opportunity to indicate any portions that should not be quoted or paraphrased in reports, publications, or presentations. *I understand that this may include the entire transcript.*

Unless I indicate otherwise after reviewing my interview transcript, I grant permission for the investigators to:

- <u>paraphrase</u> the issues raised during my interview in reports, publications, or presentations based on this study. [   ]
- <u>quote directly from my interview transcript</u> in reports, publications, or presentations based on this study:
    - without attribution [   ]
    - attributing quotations in an indirect form (e.g. Gen, Land Forces) []
    - attributing quotations to me personally (e.g. Gen J Smith) [   ]

(Agreement is indicated by checking the relevant boxes e.g. [✓])

Participant's signature______________________________________ Date __________________

I grant permission to the principal investigator to retain my raw data after the completion of this study. I understand that if I do not provide this permission, the raw data will be destroyed 8 months after the date of the interview.

Participant's signature____________________________________ Date ________________

I grant permission for the principal investigator to deposit a transcript of my interview with the National Archives of Canada for release 15 years from the date of this interview.

Participant's signature____________________________________ Date _________________

Annex C:

Interview Protocol
(Topic Categories and Sample Questions/Probes)

Introductory Remarks

- Introduce myself, explain who I am, general purpose of the research, its relevance and potential benefit to the military, why I am conducting the interview, general format of the interview and time commitment.

- Review of confidentiality/anonymity (i.e., something you say or part of your experience may be documented in a report, but no identifying information will be included).

- Review terms indicated on Voluntary Consent Form.

- Ask if any questions or if any clarification is needed.

Experiences with Networked Operations

- Overview of Canadian Forces career - occupation, training and experience, postings, rank (report dates for enrolment, occupation transfers, all training, postings, promotions, and other historical aspects of the CF career).

Interview subject's level of understanding

To begin, we will gather information related to how the interview subject understands the concept of NEOps or Network Centric Warfare (NCW). The questions that follow should guide this section of the interview.

- Please outline your personal understanding of the terms NCW and NEOps indicating what you believe to be the main similarities and differences.
- Please read the following two definitions of network-based approaches to operations. Comment on the strengths and weaknesses of both. Do you think one has more utility to CF? If so, outline why.
    - "the conduct of military operations characterized by common intent, decentralized empowerment and shared information, enabled by appropriate culture, technology and practices."
    - "… to generate increased combat power by networking sensors, decision makers and combatants to achieve shared battlespace awareness, increased speed of command, higher operational tempo, greater lethality, increased survivability, and greater adaptability through rapid feedback loops."
- Do you believe that the assumptions and attributes that are the basis for network-based approaches are congruent with Canadian requirements like transformation, the 3D (Defence, Diplomacy, Development) approach, and the three block war?
- In your opinion, is the network-based approach to operations here for the long-term?

Questions in this sub section refer to the Canadian concept of NEOps

- Is an adequate definition of NEOps available?
- Are you comfortable that individuals have a shared understanding of the term:
    - Within CF?
    - Within DND?
    - Within the wider 3D community?
- In your opinion, is NEOps fundamental to emergent doctrine?
- How should command responsibility be apportioned in a NEOps environment?
- How should a commander determine how much information is enough in a NEOps environment?
- To what degree must a commander understand the technology upon which he is dependent in a NEOps environment?

Interview subject's experience

This set of questions is designed to solicit the subject's specific experience of working in a NEOps environment. Interviewees should focus on joint and multinational experience (interagency experience is not a focus of these questions). To seek clarity, the participant should be asked to focus on one particular operational context in this section. Although responses should relate primarily to one specific scenario , there may be questions that are answered best by drawing on diverse experiences. Subjects should be asked to point out where they are discussing an alternative operational context or making a general point.

- Describe a specific (joint and multinational) NEOps context with which you have experience in terms of the following factors: the mission, constraints, restraints, level of command and control sophistication, level of joint, combined, multinational, etc., involved. Please specify what, in your view, made this a NEOps scenario.
- Is joint / multinational interworking more or less difficult than previously in networked operations? What problems arose and how were they overcome?
- Was the level of technological sophistication of CIS uniform throughout blue forces?
- Can you describe the command and control situation that you were working under in the command circumstances you were involved with?
- Was it your experience that the amount of information provided through the technical network was sufficient, too high or too little to provide the situational awareness necessary to exercise command?
- Did the technical network sufficiently discriminate between necessary and unnecessary information? How were the parameters established to make that discrimination? Would that work in all operational tempos?
- Did the technical aspects of the networked operation aid or detract from solving difficulties?
- Based on your experience in operations where networks were involved, did you find that the technical network and the human network were of equal value to the exercise of command?
- Which network, the human or the technical, did you find had the most flexibility when change was necessary?

- Which network, the human or the technical, do you think would provide the best basis for CF transformation to build upon?
- How does one go about creating an effective social network in joint and multinational environments?
- Is the presence or absence of an effective social network a factor in the success of an operation?
- Was there any confusion evident when functioning in a NEOps environment about the alignment of authority and responsibility?
- How easy was it to share your intent, both explicit and implicit, with less familiar partners? How did the network contribute to this?
- If your answers to the previous questions have not been focused on interworking with US forces, please state whether you believe that such operations are more or less difficult in networked operations? In your experience, what problems have arisen and how were they overcome?

Interview subject's assessment of the effectiveness of current networked operation

These questions should guide this part of the interview examining the subject's assessment of the effectiveness of current networked operations based on his specific experience and what was the key factor in determining the outcome.

- At what force size and force complexity would you say that NEOps should be introduced?
- To what degree is it possible to ensure the compatibility of network technology in a joint or multinational environment?
- What style of command and control do you think is appropriate for networked operations?
- What style of leadership do you think is appropriate for networked operations?
- Network-based technology potentially provides commanders and their staffs with an increased capability to supervise and direct the forces under their command. To what extent have you made use of this capability?
- In your experience with networked operations, how adaptable has the technical network been for various types of operations? For example, in your opinion will the network function as well in a warfighting environment as in a domestic/disaster response environment?
- To what degree does personal knowledge of the source of information influence your confidence in it?

Lessons Learned

These questions should guide this part of the interview eliciting lessons learned based on the subject's experience with networked operations.

- What were the lessons learned from your experience?
- To what extent was your ability to work with networked operations impacted by your environmental affiliation? What was this impact?
- In hindsight, would you change the organizational structure that you used? Was there any time where it would have been advantageous to alter organizational structure during the operation?

- What lessons in this area might be appropriate to draw from the recent US experience in the post-hurricane command and control environment in the southern US states? Is the concept of NCW valid across the spectrum of conflict?
- What changes, if any, in organization culture might CF need to make in order to benefit fully from NEOps?
- Does the CF have appropriate processes in place to benefit fully from NEOps?
- Please comment on the roles of liaison and exchange officers. How will the requirement for / employment of these personnel be affected by NEOps?
- Did the network-based environment change the nature of your interactions with the military strategic / political strategic levels? If so, how?

Closing the Interview

- If I have further questions or would like to clarify any points later, do you have any objection to me calling you?

- Are you interested in receiving a report of the findings? (If yes, verify mailing address).

- Thank You - leave business card(s) for potential follow-up.

Biographies of Those Interviewed

BRIGADIER-GENERAL P.J. DEVLIN, OMM, MSC, CD

Brigadier-General Peter Devlin enrolled in the Canadian Forces in 1978 under the Regular Officer Training Program and was commissioned as an infantry officer into The Royal Canadian Regiment.

BGen Devlin has spent the majority of his career in the field and has served in 1, 2 and 4 Canadian Brigade Groups as well as the Special Service Force. He has commanded from the platoon to brigade group level most notably commanding 1st Battalion of The Royal Canadian Regiment (1997-1999) and 2 Canadian Mechanized Brigade Group (2002-2004). His staff assignments have included operations positions in Army Headquarters, G3 - 1 Canadian Mechanized Brigade Group, and Chief of Staff of the Canadian Forces Medical Group.

BGen Devlin has several operational tours including UN tours in Cyprus (1984-85) and the former Yugoslavia (1992), two NATO tours in Bosnia (1996-97) including one as the Canadian Battle Group Commanding Officer (1998), and most recently an International Security Assistance Force tour as Commander of the Kabul Multinational Brigade in Kabul, Afghanistan (2003-2004). His unit was awarded the Commander-in-Chief Citation for opening the Sarajevo airport in 1992, and he was awarded the Meritorious Service Cross in October 2004 for his efforts in Afghanistan.

BGen Devlin is a graduate of the University of Western Ontario, the Canadian Forces Staff School, the Canadian Land Forces Command and Staff College, and the Canadian Forces College (Command and Staff Course and Advanced Military Studies Course), and the U.S. Army War College in Carlisle, Pennsylvania. He is Canadian and German parachute qualified. BGen Devlin was appointed to the Order of Military Merit in December 1997.

VICE-ADMIRAL J.C.J.Y. FORCIER, CMM, CD

Born in Trois-Rivières, Québec on 11 November 1954, Vice-Admiral Forcier joined the Navy in December 1971. On completion of basic military, as well as initial naval training, he was posted to Halifax to commence his sea-going career. He has served in HMCS SASKATCHEWAN, OTTAWA, PROTECTEUR, PRESERVER and ALGONQUIN. He eventually commanded HMCS ALGONQUIN in Halifax and Maritime Operations Group Four in Victoria.

During the 1990-91 Persian Gulf crisis, he was seconded for six months as Deputy Chief of Staff Operations with the Canadian Naval Task Group and later with the Canadian Forces Middle East Headquarters in Bahrain, for which he was "Mentioned in Dispatch".

His other postings included Staff Weapons Officer First Canadian Destroyer Squadron, Maritime Requirements Programme Coordinator at National Defence Headquarters (NDHQ), Deputy Commander Naval Reserve, Chief of Staff Joint Operations, and Director General Maritime Personnel and Operations at NDHQ.

Vice-Admiral Forcier is a graduate of Canadian Forces Command and Staff College (1988), and National Defence College (1994); he also received a Masters Degree in Leadership and Training from Royal Roads University (2000). He was invested in the Order of Military Merit in the grade of Officer in 1999 and promoted to the rank of Commander within the Order in 2005.

Vice-Admiral Forcier was promoted to the rank of Rear-Admiral in June 2003 and appointed as Commander Maritime Forces Pacific. Following his work on the Chief of Defence Staff Action Team for Transformation, Vice-Admiral Forcier was promoted to his present rank and assumed the position of Commander Canada Command on 1 July 2005.

REAR-ADMIRAL R. GIROUARD, OMM, CD

Rear-Admiral Roger Girouard is originally a native of Montréal, Québec. He began his Naval service as a reserve boatswain at HMCS CARLETON in Ottawa, before joining the Regular Force as a MARS Officer Cadet in 1974. As a Sub-Lieutenant, he was awarded his Bridge Watchkeeping Certificate whilst serving in HMCS MACKENZIE in 1976 and subsequently navigated the ex-minesweeper HMCS MIRAMICHI for a year prior to being assigned to HMCS OTTAWA as a bridge watchkeeper.

Upon completion of the Destroyer Navigation Officer course in 1978, he navigated OTTAWA and participated in a Standing Naval Force Atlantic deployment. Soon after his promotion to Lieutenant(N), he navigated the training destroyer HMCS QU'APPELLE before being assigned to VENTURE, the Naval Officer Training Centre, to instruct in navigation. He completed the Combat Control Officer Course in 1984, then served as Weapons Officer aboard HMCS ALGONQUIN.

In July of 1985 he was appointed as Commanding Officer of HMCS CHALEUR. Promoted to Lieutenant-Commander in January 1986, he undertook command of HMCS MIRAMICHI. Next, he served as Officer Commanding the Maritime Command Detachment in Argentia, Newfoundland, from July 1987 to August 1989, delving into the field of oceanographic research.

After a short period in Canadian Forces Fleet School Halifax, he was appointed as Executive Officer in HMCS ATHABASKAN in January 1990. He served in that capacity until completion of the Gulf War in 1991, when he was promoted to Commander and given the opportunity to participate in the international Naval Command College. Upon graduation in 1992, he was assigned to the Personnel Branch of Maritime Command Headquarters, where he served as Senior Staff Officer for Personnel, Plans and Policies.

In July 1994 he was appointed as Commanding Officer of HMCS IROQUOIS. During his tenure, IROQUOIS completed her TRUMP project trials and transferred to full operational status in First Maritime Operations Group as flagship. Promoted to Captain in June 1996, he was assigned as the Deputy Commander Naval Reserve at the Naval Reserve Headquarters at Pointe-à-Carcy in Québec City. In August he was appointed the Assistant Chief of Staff , Plans and Operations, Maritime Forces Atlantic, Halifax. During his tenure in Halifax he assisted in the coordination of the complex efforts of OP PERSISTENCE, the CF element of the SWISSAIR 111 salvage and recovery. He also acted as the CF liaison to the families of the victims.

He was appointed as the Commander Maritime Operations Group Four, in Esquimalt BC in July 1999 and deployed in rapid succession in September of that year to East Timor as the Canadian Joint Task Force Commander of OP Toucan, Canada's contribution to the Australian-led ITERFET coalition. Promoted to Commodore in June of 2001, he went on to study full-time at Royal Roads University, completing a MA. Rear-Admiral Girouard was appointed Director General Maritime Personnel and Readiness in December 2001 and in November 2002 he was appointed Special Advisor to the Chief of Maritime Staff.

Rear-Admiral Girouard was deployed on OP APOLLO from January to June 2003. He assumed command of Canadian Fleet Pacific 5 September 2003 and was promoted to Rear-Admiral in June 2005. He was appointed Commander Maritime Forces Pacific on 25 July 2005.

BRIGADIER-GENERAL J.P.Y.D GOSSELIN, OMM, CD

Brigadier-General Daniel Gosselin enrolled in 1974, joined the Military Engineers in 1976 and was commissioned in 1979.

His early assignments included tours at CFB Ottawa, with 1 Construction Engineering Unit in Winnipeg and as Wing Construction Engineering Officer at 3 Wing Bagotville. He also served as Assistant Professor of Civil Engineering at the Royal Military College, as an exchange officer with the US Air Force at Tyndall Air Force Base in Panama City, Florida, and in various positions at Air Command Headquarters.

In 1995, he served as Deputy Contingent Commander and Commanding Officer of the National Command Element of the first Canadian Forces deployment to the UN Mission in Haiti. Shortly after completion of this tour, he became the Executive Assistant to the Chief of the Air Staff. Upon promotion to Colonel in 1998, he assumed the position of Director of Airfield Engineering at 1 Canadian Air Division Headquarters.

Between 2001 and 2003, BGen Gosselin commanded the Canadian Forces Joint Operations Group in Kingston. During his tour, he deployed to Central Command, Tampa, Florida, to serve as Chief of Staff of Joint Task Force South-West Asia during Operation APOLLO and as

Commanding Officer of the National Command Element. He was then appointed Special Assistant to the Deputy Chief of the Defence Staff. Promoted to Brigadier-General in 2004, he assumed command of the Canadian Forces College in Toronto. In March 2005, he became Leader for the CDS Action Team on Operational Capabilities, and in June he was appointed Chief of Staff for the Canadian Forces Transformation Team.

BGen Gosselin is a graduate of the CF Command and Staff Course, the Advanced Military Studies Course and the National Security Studies Course. His education includes an undergraduate degree in civil engineering (B.A.Sc., Laval) and graduate degrees in public administration (MPA, Queen's), in structural engineering and in war studies (M.A.Sc. and M.A., RMC). He is currently a doctoral candidate in military history at Queen's University. His research interests include command and control at the strategic and operational levels of war.

BGen Gosselin is a professional engineer licensed in Ontario. He was invested as an officer in the Order of Military Merit in 2004. His interests include long-distance running, golf and military history.

In January 2006, he assumed the position of Director General – International Security Policy at National Defence HQ.

COMMODORE (RETIRED) ERIC LERHE

Commodore Eric Lerhe (Retired) joined the Canadian Forces in 1967 as an Officer Cadet at College Militaire Royal de St. Jean, Quebec, and the Royal Military College in Kingston, Ontario. He was commissioned as a Sub-Lieutenant under the Direct Entry Officer program in 1972. He then joined HMCS *Restigouche* in Esquimalt, British Columbia, where he served as the Communications and Electronic Warfare Officer. In 1975, Lieutenant Lerhe joined HMCS *Yukon* as the Deck Officer. This was followed with his posting to HMCS *Fraser* as the Weapons Officer where he remained until 1979 when he attended the Combat Control Officers course. From 1980 to 1983, he served as the Operations Officer in HMCS *Annapolis*. Upon his promotion to Lieutenant-Commander in 1983, he joined the Fifth Canadian Destroyer Squadron staff as Squadron Weapons Officer. In 1985, Lieutenant-Commander Lerhe went to Maritime Command Headquarters as Staff Officer Combat Control Readiness. During this time he also attended the Armed Forces College in Norfolk, Virginia. He was promoted to Commander in January 1986, and assumed command of HMCS *Nipigon* in September 1987. Commander Lerhe was then appointed Commanding Officer of HMCS *Saguenay* on 6 January 1989, and remained there until July 1990. He then took up duties on the staff of the Canadian Forces Command and Staff College in Toronto, Ontario. In July 1992, he was promoted to Captain (N) and assumed the position of Director Maritime Force Development in NDHQ. This was followed by his selection to attend post-graduate training at Dalhousie University in 1994. He graduated with an MA in International and Security Studies in 1996 prior to taking up his appointment as Director NATO Policy at NDHQ. In January 1998 he was named as the Commanding Officer of the Canadian Forces Maritime Warfare Centre in Halifax. He was promoted to Commodore and appointed Commander Canadian Fleet Pacific in January 2001. In that role we was a Task Group

Commander in the Persian Gulf during Operation Apollo (Canada’s contribution to the Global War on Terror) in 2002. His achievements included the capture of four al Qaeda members and making significant improvements in coalition C4I interoperability. Commodore Lerhe retired from the Canadian Forces in 2003 and is currently pursuing a PhD in political science at Dalhousie University.

MAJOR-GENERAL W.J. NATYNCZYK, OMM, CD

MGen Natynczyk joined the Canadian Forces in August 1975. He attended Royal Roads Military College and Collège militaire royal du Canada graduating with a Business Administration degree in 1979. His formative years were spent on NATO duty in Germany with The Royal Canadian Dragoons (RCD) in troop command and staff appointments.

Returning to Canada in 1983, MGen Natynczyk assumed duties as a Squadron Commander at the Royal Military College in Kingston, Ontario. In 1986, he commenced a five-year regimental tour in Petawawa, serving in several staff and squadron command appointments. The tour also included six months of UN peacekeeping duties in Cyprus.

Following attendance at Canadian Forces Command and Staff College, he served on the Army Staff in St Hubert Quebec focused on Reserve Enhancement and the Land Force Restructure staffs. In May 1994, MGen Natynczyk embarked upon a yearlong tour with the United Nations in the Former Yugoslavia. For the first half he was assigned as the Sector South-West Chief of Operations in Bosnia and Herzegovina working within 7 (UK) Armoured Brigade. For the latter half of his tour, he was assigned as the Chief of Land Operations, UNPROFOR HQ in Zagreb, Croatia.

In June 1995 MGen Natynczyk was assigned to the Vice Chief of Defence staff within National Defence HQ in Ottawa followed by command of his regiment, The RCD. The highlight of his tour was the Regiment's deployment on domestic operations in the Ottawa region during the 1997 Ice Storm. MGen Natynczyk returned to Bosnia in 1998 as the Canadian Contingent Commander. On his return to Ottawa in March 1999 he was appointed J3 Operations where he was involved in planning Canada's contributions to the Kosovo campaign, and UN operations in East Timor and Eritrea.

MGen Natynczyk was a member of the Centennial Class of the U.S. Army War College graduating in June 2002 before assuming his appointment as Deputy Commanding General, III Corps and Fort Hood. In January 2004, he deployed with III Corps in support of Operation Iraqi Freedom to Baghdad, Iraq, serving first as the Deputy Director of Strategy, Policy and Plans and subsequently as the Deputy Commanding General of the Multi-National Corps Iraq. Major-General Natynczyk assumed command of the Land Force Doctrine and Training System on 15 February 2005.

After a short tour of command, MGen Natynczyk was appointed as Chief of Canadian Forces Transformation on 1 June 2005.

COLONEL P.B. STOGRAN, MSC, CD

Colonel Stogran spent his teenage years in Richmond, B.C. before attending Royal Roads Military College in August 1976. Graduating from the Royal Military College of Canada in 1980 with a degree in Electrical Engineering, he was posted to the Third Battalion Princess Patricia's Canadian Light Infantry in Victoria. During this time, he was employed as a Rifle Platoon Commander for two years, Mortar Platoon Commander for three years, and completed his tour as Operations Captain.

In January of 1986, Colonel Stogran attended Division I of the Technical Staff Course at the Royal Military College of Sciences in Shrivenham, England. The following year, he joined the Light Armoured Vehicle Project Office in Ottawa where he participated in drafting the formal Statement of Requirement that led to the recent acquisitions of the Coyote and LAV III. A tour with the Canadian Airborne Regiment was to follow, cut short by promotion to major and a subsequent posting to the First Battalion Princess Patricia's Canadian Light Infantry in Calgary to be a Mechanized Company Commander. He served in this capacity for three years during which time his company participated in training in dismounted operations in Norway, urban warfare in the United States, and mountain operations in the Rockies. This was followed by a yearlong secondment to the United Nations as a Military Observer in Bosnia where, as the Team Leader in the enclave of Gorazde during the Serbian offensive of April 1994, he was Mentioned-in-Dispatch for courage under fire.

Upon returning to Canada in 1994, Colonel Stogran attended the Canadian Forces Command and Staff College. In July 1995, he was posted to the Australian Army Land Warfare Centre. As a formation-level tactics instructor, Colonel Stogran was the subject matter expert in manoeuvre warfare theory, mechanized operations, and non-combatant evacuation operations.

Promoted to Lieutenant-Colonel Stogran returned to Canada and took up a position with the Department of Applied Military Sciences at the Royal Military College in Kingston, Ont. As a Directing Staff instructing military technologies and project management on the Land Force Technical Staff Program, Coloenl Stogran was personally responsible for the preparation and delivery of all aspects of the Modern Weapons and Military Vehicles Courses. Colonel Stogran is licensed as a Professional Engineer in the province of Ontario.

Colonel Stogran assumed command of 3 PPCLI in September 2000. The Battalion became the Immediate Reaction Force (Land) in April 2001 and deployed to Afghanistan on Operation APOLLO/ENDURING FREEDOM in February 2002, marking the first time Canada has committed to ground combat operations since the Korean War. During the tour the Battalion launched the first combat air assault mission in the history of the Canadian Army and conducted numerous defensive and offensive combat missions at section, platoon, company and battle group level.

After returning from Afghanistan, Colonel Stogran was posted to National Defence Headquarters with the Land Staff. In April 04 Col Stogran was posted to Kingston to his present position

Much of Colonel Stogran's spare time is consumed by his passion for martial arts and related training, as he holds a second degree black belt in Karate with over thirty years of experience internationally. However, the source of his greatest enjoyment is quality time spent with his family.

BRIGADIER-GENERAL D.C. TABBERNOR, OMM, CD

Brigadier General Dennis C. Tabbernor started his military career as a Reservist with The Royal Winnipeg Rifles in September 1967. He spent five years with the Rifles serving as a Rifleman, Corporal, Senior Corporal, Second Lieutenant and Lieutenant. In May 1972, he transferred to the Regular Force. Upon completion of Infantry training he was posted to Third Battalion, The Royal Canadian Regiment in Petawawa as a Platoon Commander, where he served until 1975.

Subsequent Regimental employment included Platoon Commander and Company Second-in-Command with The Canadian Airborne Regiment in Edmonton and Petawawa; Company Second-in Command, Third Battalion, The Royal Canadian Regiment, Germany; Company Commander, First Battalion, The Royal Canadian Regiment, London, and Commanding Officer the Lake Superior Scottish Regiment, Thunder Bay.

Extra Regimental Duty included: instructor at the Infantry School, Gagetown; Aide to the Commander, The Combat Training Centre, Gagetown; SO 2 Operations, Headquarters Canadian Forces Europe, Germany; and J3 Coordination, National Defence Headquarters.

In June 1993, Brigadier General Tabbernor transferred to the Reserve Force returning to Winnipeg where he was employed at Manitoba-Lakehead District Headquarters as Senior Staff Officer Administration and Senior Staff Officer Training. In November 1994, he assumed command of his original Regiment, The Royal Winnipeg Rifles. A year later, he was promoted to Colonel and appointed Commander of Manitoba-Lakehead District and subsequently appointed Commander of 38 Canadian Brigade Group upon its formation on 1 April 1997. In July 1999, he was appointed Assistant Chief of Staff Land Force Western Area and in March 2000, was posted with the Stabilization Force (SFOR) in Bosnia Herzegovina as Assistant Chief of Staff Operations in Headquarters Multi National Division (South West). In September 2000, he was promoted to his present rank and appointed Deputy Commander Land Force Western Area. In April 2003, he was appointed Commander Canadian Joint Task Force South West Asia. He took over his present duties as Director General Land Reserve in November 2003.

He is a graduate of the Canadian Forces Staff School, the Canadian Land Forces Command and Staff College, the Canadian Forces Command and Staff College, the Advanced Military Studies Course and the National Security Studies Course.

DOCUMENT CONTROL DATA

(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document, Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's document, or tasking agency, are entered in section 8.)

Publishing: DRDC Toronto

Performing: KMG Associates. 83 Gore St, Kingston, ON K7L 2L4

Monitoring:

Contracting: DRDC Toronto

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification is indicated by the appropriate abbreviation (S, C, R, or U) in parenthesis at the end of the title)

Network enabled operations: The experiences of senior Canadian commanders (U)
Les opérations facilitées par réseaux : Les expériences des commandants supérieurs Canadiens

4. AUTHORS (First name, middle initial and last name. If military, show rank, e.g. Maj. John E. Doe.)

Joe Sharpe; Allan English

5. DATE OF PUBLICATION (Month and year of publication of document.)

June 2006

6a NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

64

6b. NO. OF REFS (Total cited in document.)

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of document, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The names of the department project office or laboratory sponsoring the research and development − include address.)

Sponsoring:

Tasking:

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant under which the document was written. Please specify whether project or grant.)

16kj01

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7711−04−7908−04

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document)

DRDC Toronto CR 2006−112

10b. OTHER DOCUMENT NO(s). (Any other numbers under which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on the dissemination of the document, other than those imposed by security classification.)

Unlimited distribution

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11), However, when further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited announcement

DOCUMENT CONTROL DATA

(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

(U) In order to fully understand the nature of Networked Enabled Operations (NEOps) today, how Canadian networked operations differ from those in other countries and how NEOps might evolve in the future, it is essential to provide context for and to document recent Canadian experiences with networked operations. However, to date, very little has been written on the Canadian experience with NEOps, particularly at the operational level of command. A recent DRDC Contract Report, “Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation,” provided some context for NEOps and noted that Canada has made significant contributions to the evolution of networked operations. It also noted that these contributions have not been well documented. This report begins the documentation of recent Canadian experiences with networked operations based on an analysis of interviews conducted during January and February 2006 with eight Canadian commanders who had recent experience with networked operations at the operational level of command. The analysis begins with a context for understanding NEOps; it then presents key issues raised in the interviews in a thematic format; and the analysis concludes by summarizing and synthesizing the key issues raised in the interviews.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

(U) Networked Enabled Operations; Canadian Experiences